

Análisis de las prestaciones del acceso al medio CSMA en redes WIFI

Trabajo Final de Grado



UNIVERSIDAD CARLOS III DE MADRID

Autor: Álvaro Arnanz Arroyo

Tutora: Ana García Armada

Departamento: Teoría de la señal y comunicaciones

Titulación: Grado de Ingeniería de Sistemas de Comunicaciones





Trabajo Final De Grado

Análisis de las prestaciones del acceso al medio CSMA en redes WIFI

Autor

Álvaro Arnanz Arroyo

Tutora

Ana García Armada

Realizado el acto de defensa y lectura del Trabajo Final de Grado el día 6 de marzo de 2015 en Leganés, en la escuela Politécnica Superior de la Universidad Carlos III de Madrid, el tribunal:

Presidente:

Secretario:

Vocal:

Acuerdan otorgarle la calificación de:

Calificación:





AGRADECIMIENTOS

A mis padres Samuel y María José,

A Mi Hermana Gema y a Lucía.

ABREVIATURAS Y ACRONIMOS

AP	Access point
CRC	Cyclic redundancy code
CSMA/CA	Carrier sense multiple access with collision avoidance
CTS	Clear to send
CW	Contention window
DIFS space	Distributed (coordination function) interframe
EIFS	Extended interframe space
IFS	Interframe space
MAC	Medium access control
MPDU	MAC protocol data unit
NAV	Network allocation vector
OFDM	Orthogonal frequency division multiplexing
PCF	Point coordination function
PDU	Protocol data unit
PHY	Physical layer
QoS	Quality of service
RIFS	Reduced interframe space
SIFS	Short interframe space
SRC	Short retry count
STA	Estación



WLAN	Wireless local area network
WEP	Wired equivalent privacy
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance

ÍNDICE DE FIGURAS

Figura 1 Esquema detallado.....	- 15 -
Figura 2 Mecanismo DCF.....	- 24 -
Figura 3 Incremento exponencial de CW	- 29 -
Figura 4 Gaps's Temporales.....	- 33 -
Figura 5 Formato de la trama MAC.....	- 34 -
Figura 6 Tiempos de Contienda	- 39 -
Figura 7 Mecanismo de backoff	- 39 -
Figura 8 relaciones temporales	- 42 -
Figura 9 descripción elementos temporales.....	- 43 -
Figura 10 cadena de bianchi-markov	- 49 -
Figura 11 throughput teórico	- 52 -
Figura 12 modelo simulador ns2	- 53 -
Figura 13 modelo simulador ns2	- 54 -
Figura 14 máquina virtual	- 55 -
Figura 15 ejecutar simulador	- 56 -
Figura 16 nam	- 56 -
Figura 17 topología de red Figura 18 tráfico generado	- 57 -
Figura 19 tráfico generado 2	- 57 -
Figura 20 archivo traza.....	- 58 -
Figura 21 herramienta tracegraph.....	- 59 -
Figura 22 resumen de red simulada.....	- 60 -
Figura 23 descarte de paquetes 1.....	- 63 -
Figura 24 descarte de paquetes 2.....	- 64 -
Figura 25 descarte de paquetes 3.....	- 65 -
Figura 26 Descarte de paquetes 4	- 66 -
Figura 27 Evolución temporal 1	- 67 -

Figura 28 evolución temporal 2	- 68 -
Figura 29 evolución temporal 3	- 68 -
Figura 30 evolución temporal 4	- 69 -
Figura 31 Eficiencia Slot Time.....	- 71 -
Figura 32 eficiencia slot time 2	- 72 -
Figura 33 Eficiencia slot time 3	- 73 -
Figura 34 comparativa slot time	- 74 -
Figura 35 relaciones temporales	- 75 -
Figura 36 relaciones temporales 2	- 76 -
Figura 37 comparativa sifs	- 77 -
Figura 38 comparativa número de usuarios.....	- 78 -
Figura 39 eficiencia 7 estaciones	- 80 -
Figura 40 eficiencia 15 estaciones	- 81 -
Figura 41 comparativa modelos	- 83 -
Figura 42 comparativa modelos 2	- 84 -

ÍNDICE DE TABLAS

Tabla 1 Campos de la trama MAC	- 35 -
Tabla 2 parámetros de simulación	- 61 -

ÍNDICE

Agradecimientos.....	- 5 -
Abreviaturas y Acronimos.....	- 6 -
Índice de figuras.....	- 8 -
Índice de tablas.....	- 9 -
Índice	- 10 -
1. Resumen	- 12 -
2. Introducción.....	- 14 -
2.1. Objetivos.....	- 15 -
2.2. Planificación.....	- 16 -
2.2.1. Diagrama de Gantt.....	- 17 -
2.2.2. Diagrama de RED	- 18 -
2.3. Marco Conceptual.....	- 19 -
2.3.1. 802.11b.....	- 19 -
2.3.2. 802.11g.....	- 19 -
2.3.3. 802.11n.....	- 19 -
3. Tipos de protocolos.....	- 16 -
3.1. Protocolos de asignación fija.....	- 16 -
3.1.1. TDMA.....	- 16 -
3.1.2. FDMA.....	- 16 -
3.1.3. CDMA.....	- 17 -
3.2. Protocolos de contienda.....	- 17 -
3.2.1. Aloha	- 18 -
3.2.2. CSMA.....	- 18 -
4. Modelo de capas de 802.11	- 21 -
4.1. Capa física.....	- 21 -
4.2. Capa de enlace de datos.....	- 22 -
5. Capa MAC.....	- 23 -
5.1. Descripción.....	- 23 -
5.2. Arquitectura de la capa MAC.....	- 24 -
5.3. DCF.....	- 25 -
5.3.1. Conceptos Básicos de la DCF	- 26 -
5.3.2. Retry Counter:	- 26 -
5.3.3. Slot Time:.....	- 26 -

5.3.4.	Interframe Spacing:	- 27 -
5.3.5.	Contador de Backoff.....	- 27 -
5.4.	Análisis de la capa MAC	- 30 -
5.5.	IFS (Interframe Spacing).....	- 32 -
5.6.	Formato De La Trama MAC.....	- 33 -
6.	Procedimiento para el acceso DCF	- 38 -
6.1.	Acceso Básico.....	- 38 -
6.2.	Procedimiento de Backoff.....	- 39 -
6.3.	Procedimientos de recuperación y límites de retransmisión.	- 41 -
6.4.	Relaciones de tiempo para la DCF.....	- 42 -
6.4.1.	Slot time.....	- 43 -
6.4.2.	Interframe Spacing.....	- 44 -
6.5.	Conclusión Acceso DCF	- 46 -
6.5.1.	Reglas específicas del estándar 802.11.....	- 46 -
6.5.2.	Reglas específicas de la DCF.....	- 47 -
6.6.	Modelo Teórico de la DCF	- 48 -
6.6.1.	Cadena de Markov.....	- 49 -
7.	Simulación de estándar WIFI 802.11.....	- 53 -
7.1.	Simulador NS2	- 53 -
7.2.	Instalación del simulador.....	- 55 -
7.3.	Aplicaciones Adicionales.....	- 56 -
7.4.	Parámetros de la simulación.....	- 61 -
8.	Simulaciones de la DCF	- 62 -
8.1.	Ventana de contención	- 62 -
8.2.	Throughput y goodput.....	- 70 -
8.3.	Slot Time	- 71 -
8.4.	SIFS (Short interframe space)	- 75 -
8.5.	Número de usuarios	- 78 -
8.6.	Comparativa de modelo teórico y simulado.....	- 83 -
9.	Conclusiones	- 86 -
10.	Trabajo futuro.....	- 88 -
11.	Bibliografía.....	- 89 -
12.	Anexos.....	- 90 -
12.1.	Código de la simulación.	- 90 -

1. RESUMEN

En este trabajo se realizará un profundo estudio sobre la capa de acceso al medio (MAC) de la tecnología WIFI (Wireless – fidelity) así como de las técnicas de control de acceso que se emplean para el control de los usuarios que acceden al sistema.

Para llevar a cabo el estudio del sistema propuesto, el trabajo ha sido estructurado en los siguientes bloques principales.

1. Estudio teórico

Se estudiarán los tipos de protocolos de acceso al medio existentes para redes inalámbricas y se abarcará el estudio fundamental del protocolo de contienda CSMA.

Para poder comprender su funcionamiento, el trabajo se basará en el estándar WIFI 802.11[1] , el cual recoge las definiciones e influencia de los parámetros fundamentales que rigen el acceso al canal inalámbrico compartido.

La capa de acceso al medio (MAC) está basada en el protocolo de acceso de la DCF el cual hace referencia a CSMA . Es en esta capa del nivel de enlace, donde nos centraremos para estudiar los parámetros fundamentales como: contador de backoff, ventana de contención, slot time o espacio entre tramas (SIFS).

Tras el estudio de dichos parámetros, procederemos a comprobar su influencia en las prestaciones del sistema mediante los siguientes datos objetivos.

- Tasa de descarte de paquetes.
- Goodput de la línea.
- Throughput de la línea.
- Número de usuarios en el sistema.

2. Modelado teórico.

Mediante el modelo teórico basado en el estudio de Giuseppe Bianchi [2] sobre el análisis de las prestaciones de la DCF, se obtendrán unos resultados teóricos sobre las prestaciones que el estándar WIFI 802.11 ofrece.

Por otra parte, proporcionará una base de trabajo enfocada a las simulaciones que se realizarán posteriormente.

3. Simulación de parámetros bajo estudio.

Tras el estudio teórico, se procederá a realizar una simulación mediante el software *NS2* (Network Simulator), desarrollado para el ámbito de las redes telemáticas [2]. Dicha simulación permitirá programar en lenguaje propio TCL, una red inalámbrica que opera bajo el protocolo CSMA y a su vez, redefinir los valores de las variables que influyen en las prestaciones finales del sistema descrito.

El objetivo fundamental de la simulación mediante un software especializado es, obtener un modelo visual y representativo de la influencia, tanto conjunta como individual, de los parámetros anteriormente descritos, para determinar la repercusión de cada uno de ellos en las prestaciones finales.

4. Comparativa de modelos.

Como parte final del trabajo desarrollado, se concluirá validando los resultados obtenidos en las simulaciones, contrastándolos con el modelo teórico expuesto y visualizando, numérica y gráficamente la variación en las prestaciones del protocolo de contienda CSMA tanto de forma teórica como práctica.

2. INTRODUCCIÓN

El estándar 802.11, comúnmente denominado WIFI (Wireless fidelity) ha representado una evolución en las comunicaciones de datos de alta velocidad y se define como una tecnología de transmisión de datos de forma inalámbrica empleando el espectro radioeléctrico en vez de un medio de transmisión guiado.

Dicha tecnología ha sufrido una gran expansión, por ello en 1999 se creó la alianza WECA (Wireless Ethernet Compatibility Alliance) con el fin de fomentar la compatibilidad del acceso inalámbrico mediante la norma 802.11 del IEEE.

A través de sus diferentes revisiones como a, b y n, ésta tecnología inalámbrica ha ido evolucionando para ofrecer mejores prestaciones en cuanto a velocidad de transmisión y robustez del sistema llegando a equipararse a su principal alternativa como es el medio de transmisión guiado del cable o fibra óptica.

La tecnología WIFI otorga como principal característica la movilidad, ya que rompe con los estándares de comunicación tradicionales y permite la interconexión de todo tipo de dispositivos como PC, dispositivos móviles personales y PDA sin uso de cableado y a su vez la fácil instalación que ofrece, al no existir una conexión física entre los dispositivos que conforman la red.

2.1. OBJETIVOS

Los objetivos principales que han motivado la realización de éste trabajo son:

- Realizar un profundo estudio en la capa MAC del estándar 802.11 IEEE
- Comprender el modelo real del acceso al medio inalámbrico.
- Comparar las simulaciones con los modelos teóricos estudiados en la carrera.
- Identificar los parámetros que regulan las prestaciones del acceso al medio Wireless.
- Estudiar las prestaciones del protocolo CSMA mediante la modificación de los parámetros fundamentales del estándar 802.11.
- Emplear documentos oficiales para el estudio realizado. (IEEE 802.11 Std)
- Recrear un escenario típico de red 802.11 IEEE mediante herramientas de simulación precisas y determinar sus prestaciones.

La consecución de los objetivos anteriormente descritos, permitirá determinar las prestaciones del sistema inalámbrico WIFI e identificar la influencia de los parámetros que rigen el acceso mediante el protocolo CSMA. A su vez se podrá estudiar la viabilidad para que los sistemas de comunicación móviles deriven tráfico a una red WIFI, como sigue en el siguiente esquema propuesto.

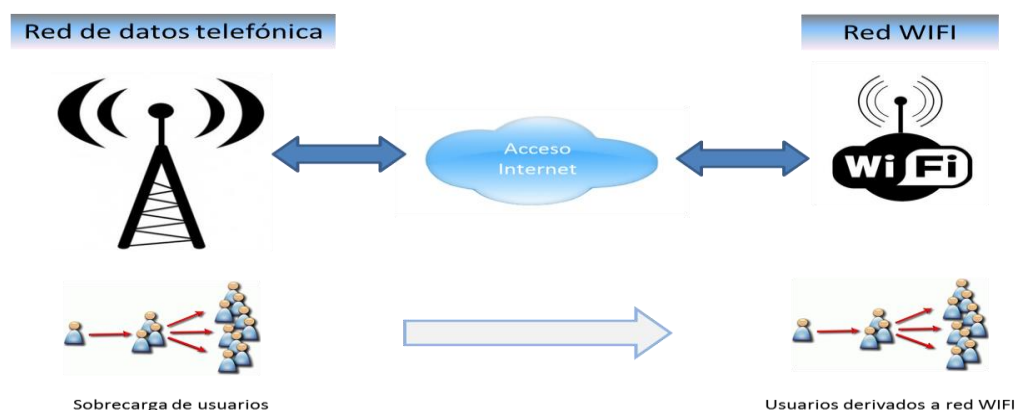


Figura 1 ESQUEMA DETALLADO

2.2. PLANIFICACIÓN

A continuación se detalla la planificación ordenada de las fases del trabajo.

Fase 1

- Identificación del propósito de estudio.
- Definir prioridades.
- Definir elementos clave bajo estudio.

Fase 2

- Búsqueda de información y material relacionado.
- Familiarización con el estudio de estándares
- Solicitar documentación
- Filtrar la información relevante para el trabajo.

Fase 3

- Estructuración del trabajo
- Realización del estudio teórico.

Fase 4

- Búsqueda de simuladores acordes a las especificaciones del trabajo.
- Elaboración de comparativa y presentación de propuestas a mi tutora.
- Elección del software de simulación para llevar a cabo el estudio.

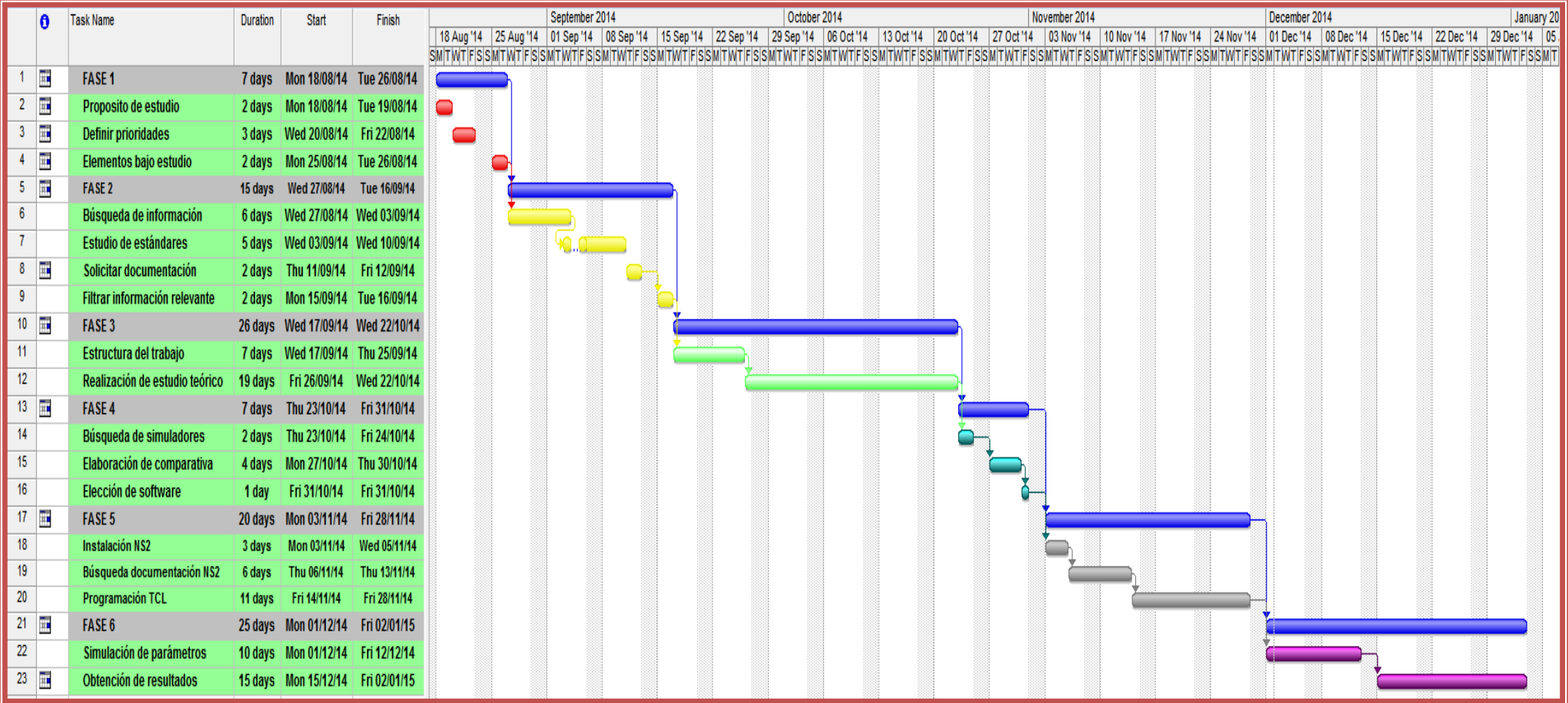
Fase 5

- Instalación y familiarización con el software escogido.
- Búsqueda de documentación para el simulador NS2.
- Familiarización con el entorno de programación TCL

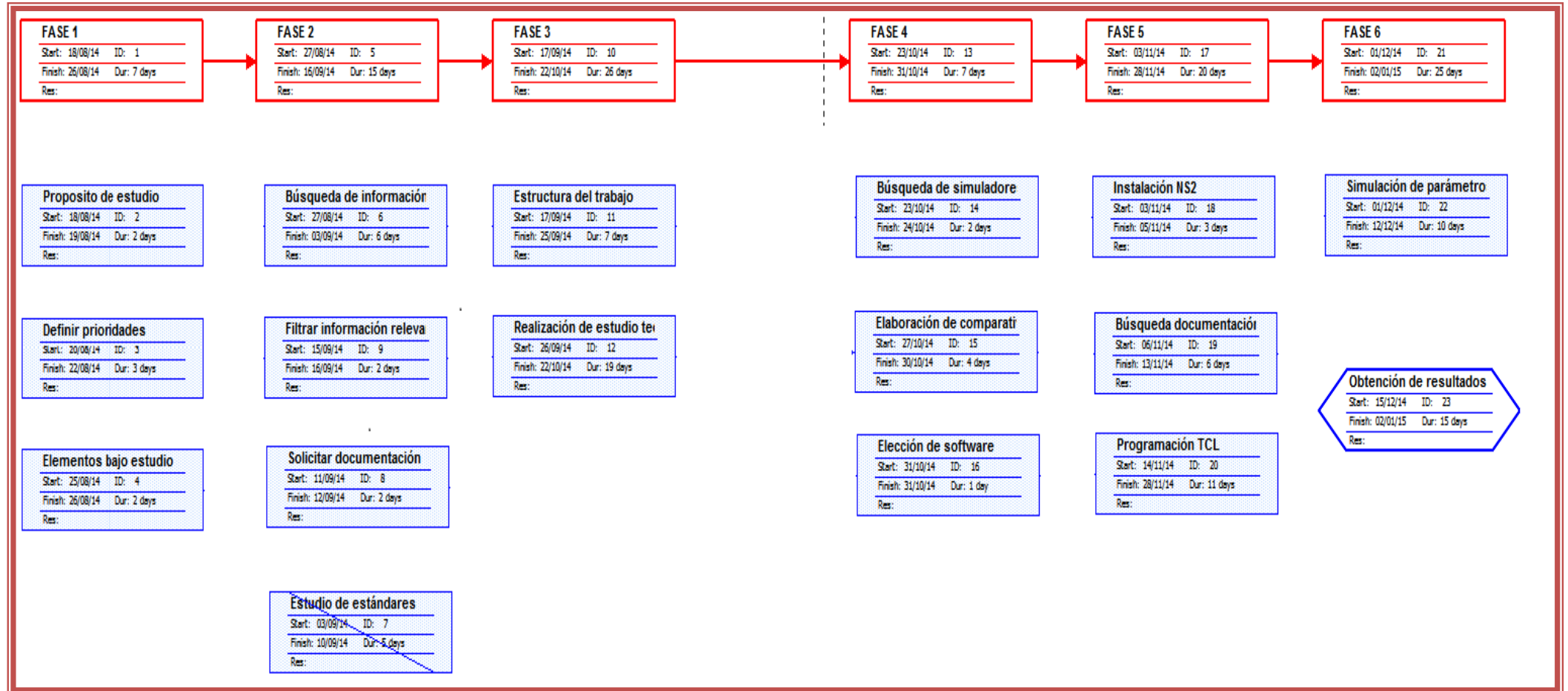
Fase 6

- Simular parámetros definidos en la fase 1
- Obtención de resultados y comparativa con valores teóricos.

2.2.1. DIAGRAMA DE GANTT



2.2.2. DIAGRAMA DE RED



2.3. MARCO CONCEPTUAL

La red inalámbrica 802.11 [1] hace referencia al protocolo de comunicación inalámbrico principalmente diseñado para redes de área local (LAN).

Las especificaciones de esta tecnología le permiten operar en las bandas no reguladas ISM (Instrumental, Científica y Médica) a 2,4 GHz sin ningún tipo de licencia.

Tras su publicación en el año 1997, se han realizado diversas modificaciones descritas a continuación:

2.3.1. 802.11b

En 1999, la IEEE crea esta nueva especificación con una velocidad teórica de 11 Mbps, la cual se ve limitada por las técnicas de acceso que emplea CSMA/CD (Carriersense Medium Access/ CollisionDetect) a 5.9 Mbps en TCP.

2.3.2. 802.11g

Creado en Junio de 2003, dicha modificación trabaja en la banda de 2.4 GHz, con una tasa binaria máxima en la capa física de 54 Mbps y 22 Mbps de throughput de media.

La ventaja de esta revisión fue la amplia compatibilidad a nivel de hardware con la revisión 802.11b.

2.3.3. 802.11n

En 2004 la IEEE anunció una nueva revisión del estándar 802.11, mejorando las especificaciones previas y aportando nuevas tecnologías como MIMO (*Multiple Input Multiple Output*).

Opera en las bandas de 2.4 GHz y 5 GHz en un rango de tasa binaria entre 54 Mbps y 600 Mbps. Dicha modificación fue aprobada en octubre de 2009.

3. TIPOS DE PROTOCOLOS

Los protocolos a continuación descritos se engloban dentro del rango de acceso a un canal compartido por múltiples usuarios, dichos protocolos reciben el nombre de Protocolos de acceso múltiple.

Se subdividen en asignación fija y de contienda.

3.1. PROTOCOLOS DE ASIGNACIÓN FIJA

3.1.1. TDMA

El acceso múltiple en el TDMA se realiza mediante la asignación de un slot temporal a cada usuario para que realice la transmisión durante ese intervalo.

Dicho protocolo no es aplicable al estándar 802.11 por sus características.[1][2]

3.1.2. FDMA

En dicho protocolo, se subdivide el espacio radioeléctrico en canales para el uso compartido de los usuarios, mediante la asignación de una sub-banda de todo el espectro a cada estación transmisora.

Dicho protocolo no es aplicable al estándar 802.11 por sus características.[1][2]

3.1.3. CDMA

En CDMA, las estaciones transmisoras transmiten continuamente empleando la misma frecuencia.

A cada estación se asigna una modulación en el código que es única.

Mediante dicha modulación, las estaciones receptoras son capaces de diferenciar el origen de la trama de datos recibida.

3.2. PROTOCOLOS DE CONTIENDA

Antes de la discusión de los diferentes protocolos de contención, el funcionamiento básico se rige por las siguientes reglas[2][1]:

1. Modelo de la estación transmisora: consiste en la coexistencia de N estaciones que comparten el medio inalámbrico.
2. Canal único: el canal solo estará disponible para una única estación transmisora simultáneamente.
3. Colisiones: si dos tramas se transmiten simultáneamente, se solaparán en el espacio de tiempo, produciendo la colisión de paquetes y por lo tanto será una transmisión fallida. A su vez, las estaciones pueden detectar las colisiones y retransmitirlos posteriormente.
4. La evolución temporal del canal podrá ser:
 - i) Tiempo continuo: la transmisión puede ser realizada por las estaciones en cualquier instante de tiempo.
 - ii) Tiempo ranurado: se subdivide el espacio temporal en slots, al comienzo de estos, las estaciones pueden comenzar a transmitir.

3.2.1. ALOHA

Dicho protocolo es llevado a cabo por las estaciones transmisoras mediante el envío de los paquetes de datos de los que dispongan, según sea su llegada.

Si una estación tiene datos que transmitir, los envía al medio inmediatamente, en el caso de que no reciba asentimiento de la estación receptora y venza el tiempo de time-out, se procederá a la retransmisión del mensaje completo aun cuando solo se ha destruido parte de los paquetes enviados.[1][2]

Existe una variación del protocolo Aloha, la cual se denomina ranurado, que emplea divisiones temporales donde las estaciones pueden transmitir solo al comienzo de estas.

3.2.2. CSMA

Dicho método emplea el sensado de portadora, empleado para “escuchar” el canal y poder determinar si se encuentra libre u ocupado.

Existen variaciones del protocolo CSMA:

3.2.2.1. 1-PERSISTENTE

En el momento que la estación transmisora esta lista para transmitir datos, realiza un sensado del canal y en el caso de que el canal se encuentre ocupado, continua comprobando el estado del medio hasta que detecta que se encuentra libre de colisiones (idle).[1][2]

3.2.2.2. P-PERSISTENTE

Constituye una variación del protocolo 1-persistente, empleando modelos probabilísticos.[1][2]

El emisor realiza el sensado del canal hasta que detecta el medio en estado idle, tras ello, enviará los paquetes de datos de los que disponga con una probabilidad p .

Dicho proceso se repite hasta que ocurre una colisión debido a otra estación transmisora.

3.2.2.3. CSMA NO PERSISTENTE.

Cuando el emisor se encuentra listo para iniciar la transmisión, comprueba el estado del canal.[1][2]

En el caso de que esté ocupado, se emplea un tiempo de espera aleatorio antes de volver a comprobarlo.

Si el resultado de dicha comprobación es idle, se procede al envío de los datos y en el caso de que ocurra una colisión se repite el proceso esperando un tiempo de contención aleatorio antes de volver a sensar el canal.

3.2.2.4. CSMA RANURADO

Dicha técnica mantiene similitudes con ALOHA ranurado, empleando una división en slots temporales de duración fija.[1][2]

Como se ha comentado anteriormente, la transmisión solo puede ser efectuada al comienzo de cada time slot.

Si ocurren colisiones, la estación que inicia la transmisión, espera un tiempo de contención aleatorio y vuelve a comprobar el estado del canal repitiendo el proceso.

3.2.2.5. CSMA/CD

Dicho método mantiene similitudes con CSMA 1- persistente.

Las estaciones transmisoras continuamente están comprobando el estado del medio para que, en el caso de que existan colisiones, la transmisión sea abortada lo antes posible para reducir la probabilidad de que una segunda colisión se produzca.

La mejora de este protocolo reside en la eficiencia a la hora de detectar las colisiones, evitando tiempos de espera innecesarios en la recepción de asentimientos por parte de la estación receptora ya que no es necesario esperar para detectar las colisiones.

Como gran inconveniente de este método es que se necesita un canal full-duplex para realizar simultáneamente el sensado del canal y a su vez la transmisión de los datos.[1][2]

3.2.2.6. CSMA/CA

Bajo las premisas de CSMA/CD, dicho protocolo establece nuevas reglas para tomar mayores precauciones a la hora de evitar la colisión de paquetes.

Dicho protocolo emplea la detección del canal físico y del canal virtual permitiendo una conexión full-duplex, necesaria para el funcionamiento del estándar 802.11.
[1][2]

4. MODELO DE CAPAS DE 802.11

El estándar 802.11 cubre dos capas fundamentales, las cuales son:

- Capa física (PHY)
- Capa de enlace de datos

4.1. CAPA FÍSICA

La capa física del estándar 802.11 (PHY) es la interfaz encargada de comunicar la capa MAC y el medio inalámbrico. Dicha capa comprende principalmente la modulación que emplea el sistema y la frecuencia usada por cada protocolo.

La capa física proporciona tres tipos de funcionalidades.

1. Intercambio de tramas entre la capa física y la capa de acceso al medio.
2. Emplear la portadora de la señal.
3. Modulación de la señal para transmitir tramas a través del medio y proporcionar al sistema el mecanismo de detección de portadora.

La capa física a su vez se divide en dos subcapas:

- Procedimiento de convergencia de la capa física (PLCP).
- Subcapa dependiente del medio (PMD).

La subcapa PLCP actúa en el sistema como la unión entre la capa MAC y la transmisión a través del medio. Dicha subcapa, añade cabeceras propias a la trama de datos así como el preámbulo necesario para el control de sincronismo.

La subcapa PMD es la responsable de transmitir vía inalámbrica mediante una antena, los datos que recibe de la subcapa PLCP.

Existe adicionalmente una función de la capa física denominada CCA (Clear Channel Assessment), que es la encargada de indicar a la capa MAC la presencia de una portadora para poder llevar a cabo los mecanismos de detección de señal en el medio, para gestionar las colisiones del sistema.

4.2. CAPA DE ENLACE DE DATOS

La capa de enlace de datos tiene como función principal la construcción de los paquetes que serán enviados a capas superiores y controlar el acceso al medio físico.

Dicho control de acceso, define los procesos y mecanismos para que los diferentes dispositivos puedan acceder a la red inalámbrica y comenzar el intercambio de información.

La capa de enlace de datos se divide en dos subcapas inferiores, las cuales son:

- Capa de enlace lógico (LLC)
- Capa de control de acceso al medio (MAC)

La capa de enlace lógico (LCC) añade información a la trama de datos que será enviada al nivel superior.

Esta información adicional, sirve para identificar el tipo de protocolo de la capa de red que se está empleando.

La capa de control de acceso al medio (MAC), es la encargada de proporcionar a la capa de enlace de datos, las delimitaciones en la trama que se enviará a la capa física. Esto es el comienzo y final de los datos dentro de la trama bajo los requisitos establecidos por la señalización física del medio y el tipo de protocolo empleado en la capa de enlace de datos.

Mediante el protocolo CSMA para el control de acceso al medio empleado en el estándar 802.11, la capa MAC es capaz de comunicarse con la capa física para llevar a cabo el proceso de detección de la presencia de portadora de señal y gestionar el acceso al medio de los usuarios del sistema inalámbrico.

5. CAPA MAC

Una vez descritas las capas del protocolo 802.11 WIFI, el trabajo se centrará en analizar profundamente la subcapa MAC y determinar los parámetros que regulan el acceso de los usuarios al sistema, bajo el protocolo CSMA.

La subcapa MAC constituye la parte más baja de la capa de enlace y proporciona el control para la transmisión de la información a través del medio inalámbrico.

Proporciona el mecanismo que permite asignar los recursos a los usuarios que acceden al canal.[3]

5.1. DESCRIPCIÓN

El proyecto se centra en el acceso al medio de los usuarios para poder hacer uso de la tecnología WIFI en el estándar 802.11 (Wireless Fidelity).

La capa de control de acceso al medio (MAC) es la encargada de gestionar y mantener las comunicaciones entre los dispositivos que desean acceder.

La capa MAC debe coordinar el acceso a un canal radio usando su capa física para poder detectar la portadora de la señal.

Para que se pueda establecer una comunicación, el emisor primero ha de obtener el acceso antes de poder transmitir tramas.

Debido a la naturaleza de este estándar, el medio se comporta como un canal compartido, donde múltiples usuarios acceden a él según un patrón aleatorio.

Para realizar esta tarea, el estándar 802.11 define dos métodos:

- DCF(Función de coordinación distribuida).
- PCF(Función de coordinación de punto).

En esta sección se describe el acceso condicional al medio, incluida la arquitectura de la subcapa MAC y la función de distribución coordinada (DCF).

5.2. ARQUITECTURA DE LA CAPA MAC

Se muestra a continuación una representación de la arquitectura de acceso al medio, en la cual los servicios PCF y el HCF son proporcionados usando los servicios de la función de distribución coordinada.

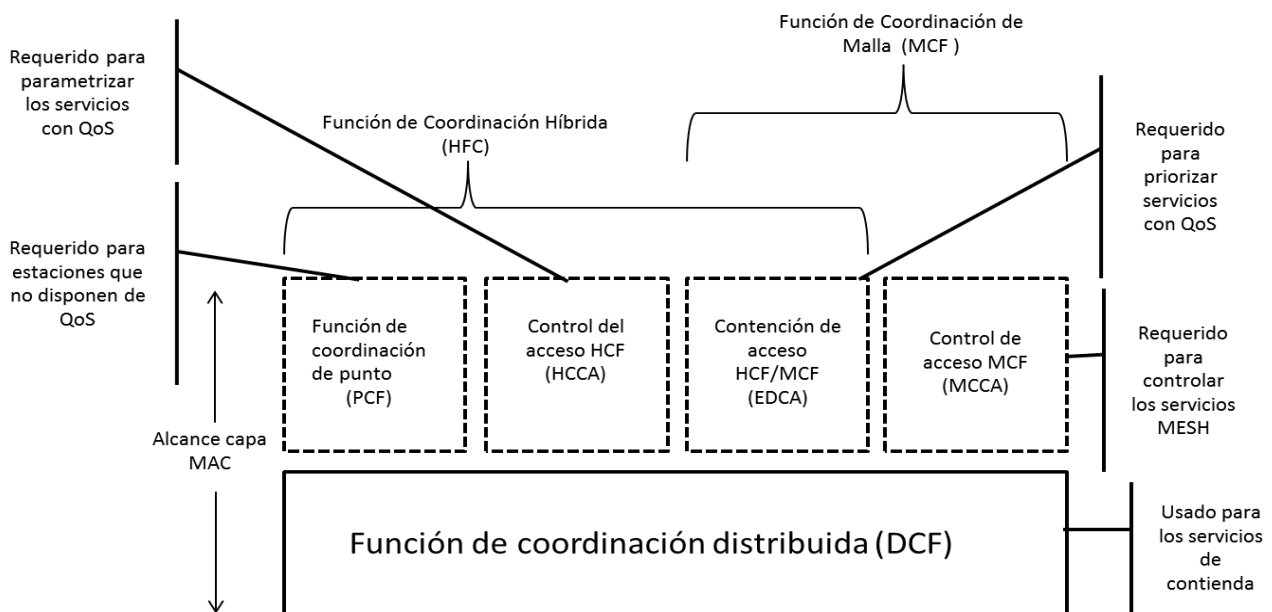


Figura 2 MECANISMO DCF

La capa MAC del estándar IEEE 802.11 WIFI define dos modos de funcionamiento, el modo de acceso distribuido DCF que utiliza el protocolo CSMA/CA y es el más empleado en los accesos vía radio comerciales; el otro modo, es el centralizado (PCF), el acceso al medio de los usuarios está libre de colisiones y se da con baja frecuencia de implementación en equipos comerciales.

A continuación basándonos en las referencias del estándar WIFI 802.11, analizaremos el método de acceso DCF y estudiaremos su protocolo CSMA/CA para generar una simulación donde N usuarios comparten el medio.[3]

5.3. DCF

Es el método de acceso fundamental de la capa MAC del estándar 802.11, el cual esta implementado en todos los STA's.:

Para que una estación pueda transmitir, primero ha de sensar el medio para determinar si otra estación está transmitiendo en dicho instante.

- Si el medio no se encuentra ocupado, se procederá a la transmisión.

El algoritmo distribuido CSMA impone que se debe respetar un gap de tiempo mínimo entre secuencias contiguas de trama.

Una estación transmisora debe verificar que el medio se encuentra *IDLE* durante este intervalo determinado de tiempo antes de intentar transmitir de nuevo.

- Si el medio se encuentra ocupado, la estación transmisora debe aplazar su transmisión hasta que finalice el envío actual por parte de otro equipo.

Tras el aplazamiento, la estación debe seleccionar un tiempo aleatorio de *backoff* y decrementar dicho contador mientras el medio se encuentre *IDLE*.

Una transmisión se considera exitosa cuando una trama de ACK (asentimiento) es recibida por la estación transmisora, la cual es procedente de la dirección del receptor (RA) o cuando el grupo de tramas han sido enviadas por completo.[3][4]

5.3.1. CONCEPTOS BÁSICOS DE LA DCF

5.3.2. Retry Counter:

El *retrycounter* es un método que se emplea para contar el número de intentos de transmisión que han sido fallidos. Su valor inicial comienza en cero y cada transmisión fallida se incrementa en una unidad.

En el caso que se alcance el valor máximo de este contador, se comienza a descartar los paquetes entrantes y las pérdidas son reportadas a capas superiores.

Existen dos tipos de contadores a su vez, los de larga duración, indicados para el mecanismo de intercambio de tramas RTS/CTS; y los de corta duración, indicados para el uso normal de paquetes empleando el método de la DCF.[3][4]

5.3.3. SLOT TIME:

Un slot time hace referencia a un slot temporal cuando las condiciones del medio son libres de colisiones.

Dicho Slot time conlleva el tiempo que el transmisor comprueba que el medio se encuentra libre de colisiones, el tiempo que el receptor emplea en devolver el asentimiento para confirmar la transmisión, el tiempo de propagación de la señal y el tiempo empleado por la MAC en gestionar dicho proceso.[3][4]

5.3.4. INTERFRAME SPACING:

El estándar 802.11 especifica seis tipos de espacio entre tramas, de las cuales, tres se emplean para el acceso al medio.

Se definen diferentes tipos de prioridad, en función del tipo de paquetes del que conste la trama a enviar.

Los paquetes con un mayor grado de prioridad, emplean un tiempo de *interframe* menor, lo cual va a repercutir en que puedan acceder al canal antes que aquellos paquetes con un menor grado.

El estándar 802.11 define el tiempo de espacio entre tramas para CSMA como el tiempo mínimo necesario que ha de permanecer el canal en un estado IDLE (libre de transmisiones) antes de que los nodos de acceso aleatorio puedan usar el canal.[3][5]

5.3.5. CONTADOR DE BACKOFF

La DCF emplea un contador de backoff exponencial para hacer frente a los intentos de transmisión fallidos.

Después de que la transmisión y el DIFS ha transcurrido, se lleva a cabo un tiempo de *backoff* o ventana de contención (CW). Dicha ventana de contención, está dividida a su vez en slots, cuya duración viene determinada por el estándar.

La estación transmisora, lleva a cabo un tiempo aleatorio de backoff y espera dicho tiempo antes de comenzar la transmisión de paquetes.

Como consecuencia de este método, si existen múltiples estaciones transmisoras intentando acceder al medio compartido para comenzar con su transmisión, aquella que disponga de un tiempo de *backoff* más bajo será la primera en acceder.

La ecuación que regula este tipo de técnica se define:

$$BC = \text{int}(\text{rnd}() * CW(k))$$

- La función $\text{rnd}()$ devuelve un valor distribuido uniformemente entre $[0, 1]$.
- $CW(k)$ representa la ventana de contención tras k intentos fallidos de transmisión.

Para el primer intento de transmisión de un paquete, el estándar 802.11 define que se asume un valor para la ventana de contención (CW) igual al valor mínimo especificado en CW_{min} .

En el caso que se produzca una colisión en la transmisión, dicho contador CW tomará un valor que será el doble hasta que alcance un valor límite que especifica el protocolo.

Tras k intentos fallidos de transmisión, la ventana de contención toma el siguiente valor.

$$CW(k) = \min(CW_{max}, 2^k * (CW_{min} - 1))$$

El valor mínimo de una ventana de contención sólo se reestablece una vez que la transmisión ha sido realizada correctamente o en el caso que el paquete se descarte.

La ventaja de permitir ventanas de contención de larga duración ayuda y permite a mantener el protocolo estable para el acceso de todos los nodos.

A continuación se muestra un ejemplo de incremento de la ventana de contención:

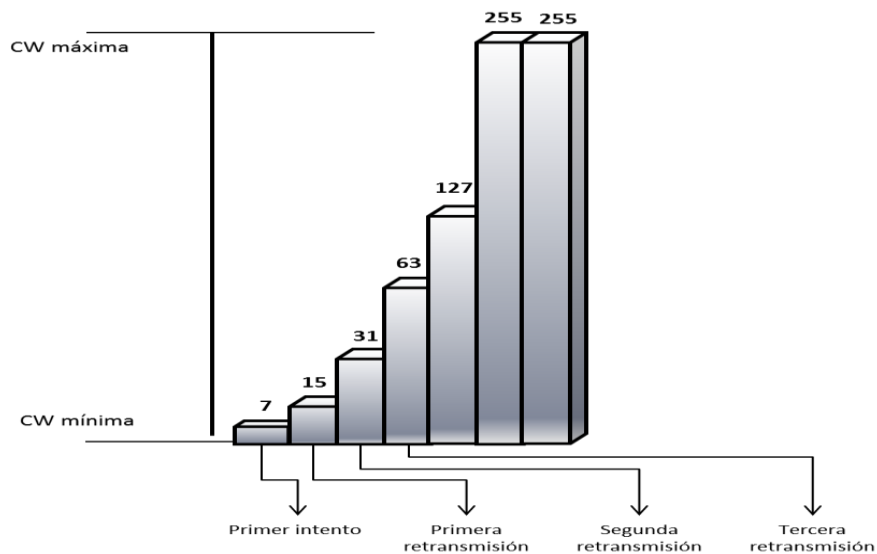


Figura 3 INCREMENTO EXPONENCIAL DE CW

El estándar permite un refinamiento de dicho método, el cual puede ser empleado bajo ciertas circunstancias, con el propósito de minimizar el número de colisiones.

Su funcionamiento consiste en que tanto la estación transmisora, como la receptora, realizan un intercambio de tramas cortas de control después de determinar que el medio está libre y después de cualquier aplazamiento o tiempo de backoff, antes de la transmisión de datos.[4][3]

5.4. ANÁLISIS DE LA CAPA MAC

A continuación se explicará con mayor profundidad el protocolo de acceso al medio CSMA, el cual será el eje central de éste proyecto, tanto en la parte teórica, como en la simulación.

El protocolo de acceso al medio básico, es un DCF que permite, para un medio automático, compartir el acceso usando CSMA/CD (Carrier Sense Multiple Access with Collision Detect) y un tiempo aleatorio de backoff que se ejecuta bajo la condición de que el medio se encuentre ocupado.

Una ventaja de este método reside en que todos los receptores, disponen de ACK positivos para indicar que la transmisión ha sido exitosa, en el caso de que no exista dicha confirmación, el emisor procederá a la retransmisión de la información por completo.

El protocolo CSMA/CD, está diseñado para reducir la probabilidad de colisión entre múltiples estaciones que acceden y comparten al medio.

Justo después de que el medio se encuentre en estado IDLE tras haber estado ocupado, es cuando sucede la mayor probabilidad de colisión. Esto es debido a que múltiples estaciones podrían encontrarse esperando a que el medio estuviera disponible de nuevo. Debido a esta situación, es necesario implementar el anteriormente citado tiempo de espera aleatorio (backoff).

Existen dos tipos de sensado de portadora, los cuales reportan a capas superiores si el canal se encuentra libre u ocupado. Estas funciones de sensado se pueden clasificar en físicas y virtuales.

Mecanismo de Sensado de Portadora:

Las funciones tanto físicas como virtuales para el sensado de portadora, son empleadas para determinar el estado en el que se encuentra el medio.

Cuando los mecanismos indican que el medio se encuentra ocupado, indica a todas las estaciones de esta situación, mientras que si no existe ninguna indicación, el medio debe considerarse en estado *Idle*.

El sensado físico de portadora es proporcionado por los componentes de RF en la capa física, donde el método empleado varía en función de la modulación y el medio.

El sensado de portadora virtual, se logra, mediante la distribución de información de reserva, ante el inminente uso del medio mediante el intercambio de tramas RTS (Request to Send) y CTS (Clear to Send) anteriores a la trama de información que realmente se quiere transmitir.

Estas tramas previas, contienen un campo de duración, el cual define el periodo de tiempo que el medio está reservado para transmitir y para el retorno del ACK.

El mecanismo de sensado de portadora virtual, el cual es en el que nos centramos en dicho trabajo, debe ser proporcionado por la capa MAC. Este mecanismo hace referencia a los NAV (*Network allocation vector*).

El NAV, mantienen una predicción del futuro tráfico que se espera, basándose en la duración de la información que es anunciada por el intercambio de tramas RTS/CTS antes del intercambio de datos. Esta duración de la información a su vez está disponible en las cabeceras de todas las tramas de la capa MAC enviadas durante el CP (*periodo de contención*).

Los mecanismos de sensado de portadora (CS) combinan el estado del NAV junto con el de los transmisores para determinar el estado *busy/idle* del medio. El NAV puede ser considerado como un contador con un paso uniforme hasta llegar a 0. Cuando dicho contador alcanza el valor de 0, el método de sensado virtual de portadora indica que el medio se encuentra en su estado *idle* y por el contrario, cuando dicho contador no es 0, indica que el medio esta en modo *busy*.

El medio debe ser detectado como ocupado en el momento que una STA se encuentra transmitiendo.

5.5. IFS (INTERFRAME SPACING)

El intervalo de tiempo entre las tramas que viajan a través del medio se denomina *interframespacing*. [3][5]

Un STA debe determinar si el medio se encuentra libre, mediante el uso de la función de sensado de portadora durante el intervalo especificado.

Existen seis tipos de espacios entre tramas que proporcionan diferentes niveles de prioridad para el acceso inalámbrico.

Dichos intervalos entre tramas se definen como sigue:

- RIFS *reduced interframe space*
- SIFS *short interframe space*
- PIFS *PCF interframe space*
- DIFS *DCF interframe space*
- AIFS *arbitration interframe space*
- EIFS *extended interframe space*

Los diferentes tiempos anteriormente descritos son independientes de la tasa de bits de las estaciones transmisoras.

Los IFS son definidos como tiempos o *GAP*'s del medio inalámbrico y son fijados por la capa física

En la siguiente imagen se observa la distribución de dichos *GAP*'s.

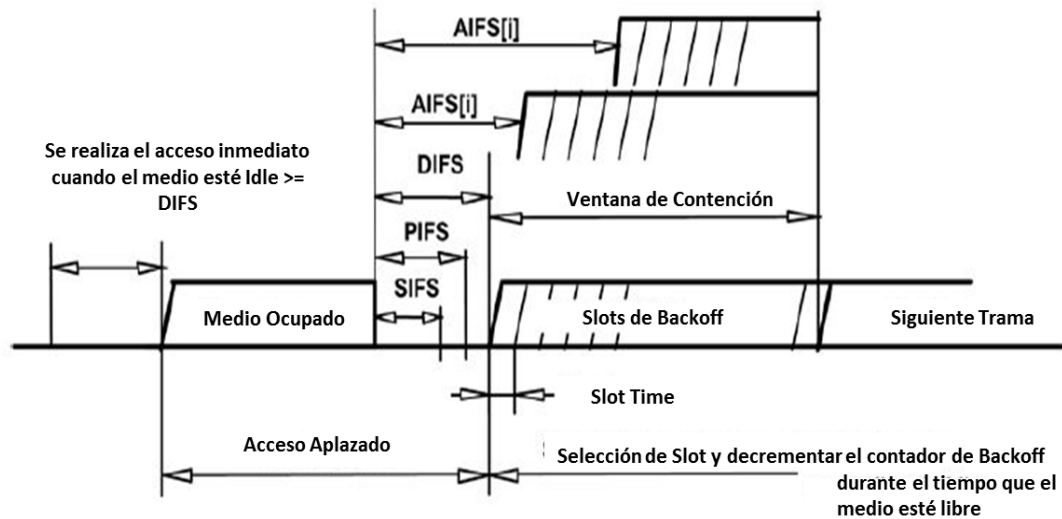


Figura 4 GAPS'S TEMPORALES

5.6. FORMATO DE LA TRAMA MAC

Mensajes

Existen tres tipos de mensajes para la capa MAC:[3][6]

- **Control:** son los mensajes encargados de verificar y controlar la correcta comunicación entre los nodos que intentan acceder al medio. Las estaciones intercambian mensajes de asentimiento para la recepción de paquetes o mensajes que indican a otras estaciones su disponibilidad para recibir paquetes si el medio está libre.
- **Datos:** son los encargados del transporte de las tramas de datos que provienen de capas superiores.

- **Management:** se pueden subdividir a su vez en aquellos destinados a la seguridad y confidencialidad y aquellos destinados al intercambio de paquetes entre las estaciones transmisoras.

Trama:

A continuación se describe el formato de la trama que rige el intercambio de información entre las estaciones transmisoras.

Todas las tramas que se intercambien deben cumplir este formato.

Componentes básicos:

Se definen tres componentes básicos en la estructura de la trama: [2]

- Una cabecera MAC, que incluya control de trama, duración, dirección e información adicional como control de información de QoS.
- Un campo de longitud variable que contenga información específica de la trama, tipo y subtipo.
- Un *framechecksequence* que contiene el CRC para la detección de errores.

A continuación se muestra el formato general de la trama MAC.

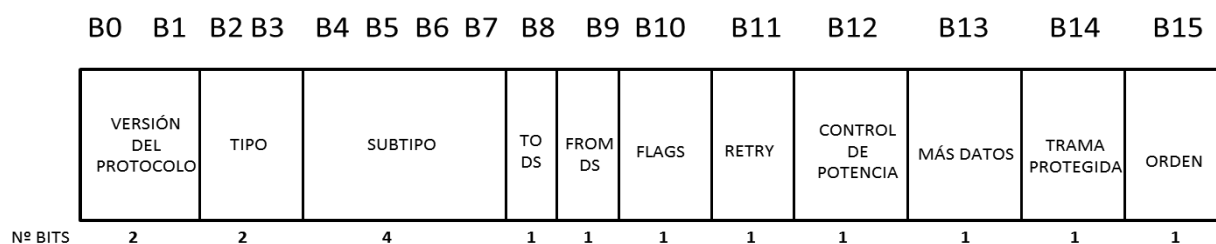


Figura 5 FORMATO DE LA TRAMA MAC

Los campos de los que consta la trama son los siguientes:

Versión de protocolo

Consta de una longitud de 2 bits y es invariante tanto en tamaño como en posición. En este protocolo su valor es el de 0 y todos los demás valores están reservados.

Tipo y subtipo

El campo de *Type* consta de 2 bits de longitud y el campo *Subtype* consta de 4 bits de longitud. Ambos campos sirven para identificar la función que tiene la trama, como se ha descrito antes puede ser de control, gestión o datos.

- 00 indica trama de management
- 01 indica trama de control
- 10 indica trama de datos
- 11 está reservado.

Cada tipo de trama, a su vez tiene diferentes subtipos que se detallan en las tablas adjuntas.

To DS y From DS

A continuación se detalla el significado de la combinación de estos campos:

TO DS y From DS	SIGNIFICADO
To DS=0 From DS=0	Una trama de datos destinada desde una STA hacia otra STA.
To DS=1 From DS=0	Una trama de datos destinada por el DS o siendo enviada por una STA.
To DS=0 From DS=1	Una trama de datos saliendo del DS o siendo enviada por la entidad de puerto de acceso en un punto de acceso.
To DS=1 From DS=1	Una trama de datos usando el formato de cabecera MAC de cuatro direcciones.

TABLA 1 CAMPOS DE LA TRAMA MAC

MF (MoreFragments)

Sirve para indicar si el paquete entrante se encuentra fragmentado al proceder de capas superiores.

En el caso que esté fragmentado se indica con el valor 1.

Retry

Sirve para indicar que las tramas que se han retransmitido, se encuentren duplicadas indicandolo con un bit a 1.

Power Management

Empleado en el uso de dispositivos portátiles, se puede desactivar parte de la interfaz de red para ahorrar energía.

More Data

Empleado para indicar si una estación transmisora dispone de más datos disponibles para alguna estación específica.

WEP

Empleado para indicar si la trama se ha codificado empleando el algoritmo WEP (*Wireless Equivalent Privacy*).

Orden

Dedicado al envío específico de paquetes ordenados en caso de que sea crucial. Consta de 1 bit de longitud y se emplea para dos propósitos.

- Es puesto a 1 cuando se transmite una trama sin QoS por una estación transmisora que no dispone de los mecanismos de QoS.
- Es puesto a 1 para indicar que la trama contiene un campo de control HG.

Duration ID

Este campo contiene 16 bits de longitud y define el tiempo que una trama ocupa el canal.

El contenido varía en función del tipo de trama y subtrama como se define a continuación.

- En tramas de control los 14 bits más significativos llevan asignados el identificador de la estación transmisora.
- En tramas transmitidas por el PC, el campo de duración se fija al valor de 32768.
- En todas las tramas enviadas por una estación sin QoS se asigna un valor en función del tipo de trama definido en los campos de tipo y subtipo.
- En tramas de datos y management contiene un valor variable en función de cómo se definan los campos de tipo y subtipo.

Address

Consta de cuatro campos en la trama MAC y cada uno de ellos a su vez consta de 48 bits.

Existen diferentes variantes:

- Dirección individual, asignada a un STA en particular.
- Dirección de grupo, la cual es una dirección multidestino.

Sequence

Consta de 16 bits y es empleada para las labores de desfragmentación y evitar la duplicidad de tramas retransmitidas. Está compuesta por dos campos, 4 bits en el número de fragmento y 12 que indican el número de secuencia.

En función de la estación transmisora, se define un número de secuencia diferente a cada trama.

Payload (Cuerpo del Mensaje)

Se encapsula dentro de la trama la carga de datos útiles, provenientes de capas superiores. La MTU o unidad máxima de datos que puede transportar es de 2304 bytes.

FCS (FrameCheckSequence)

Consiste en el mecanismo de comprobación de errores en la trama de datos mediante mecanismos de redundancia cíclica (CRC).

6. PROCEDIMIENTO PARA EL ACCESO DCF

A continuación se describe el procedimiento que las estaciones transmisoras realizan para poder compartir un medio inalámbrico basándose en la función de coordinación distribuida (DCF) cuyo método de acceso es CSMA.[3][4]

6.1. ACCESO BÁSICO.

El acceso básico se refiere al mecanismo que las estaciones transmisoras emplean para determinar si pueden comenzar una transmisión usando la DCF.

Por norma general, una estación transmisora puede transmitir una MPDU (*unidad de datos del protocolo MAC*) cuando está operando bajo el método de acceso DCF, cuando determina que el medio está idle por un periodo igual o mayor que el tiempo estipulado por DIFS.

Si se cumple dicha condición y los mecanismos de sensado de portadora (CS) determinan que el medio se encuentra ocupado en el instante que la estación transmisora comenzaría su envío, se activan los mecanismos de tiempo aleatorio de backoff y la estación inicia los mecanismos en modo de acceso básico.

Una vez detectado el medio ocupado y existiendo una colisión, la estación transmisora selecciona un tiempo aleatorio de backoff usando la ventana de congestión actual (CW).

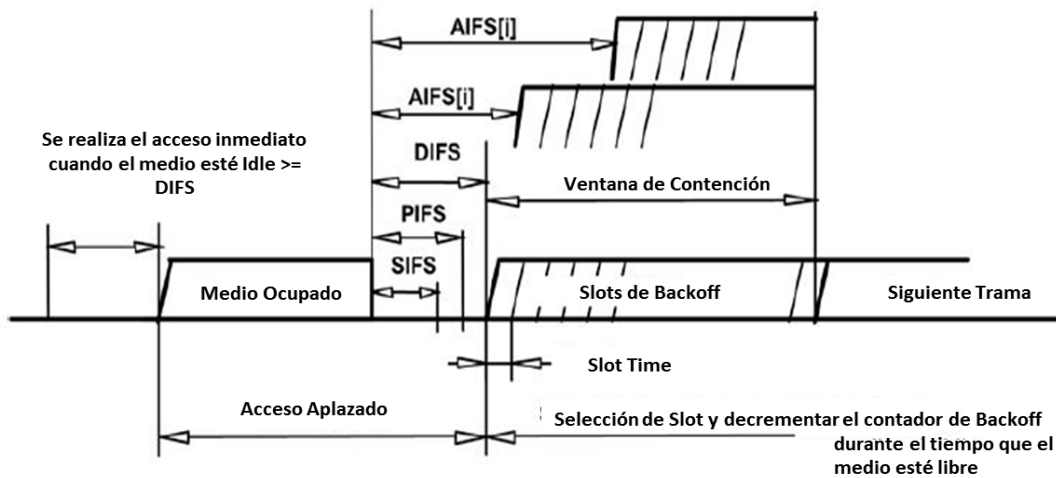


Figura 6 TIEMPOS DE CONTIENDA

6.2. PROCEDIMIENTO DE BACKOFF

Este apartado describe el procedimiento de backoff que es empleado por la DCF.

El procedimiento de backoff debe ser invocado por una estación transmisora que al intentar transmitir una trama detecta el medio en modo *busy*, indicado por los mecanismos físicos y virtuales de control de acceso.[4][3]

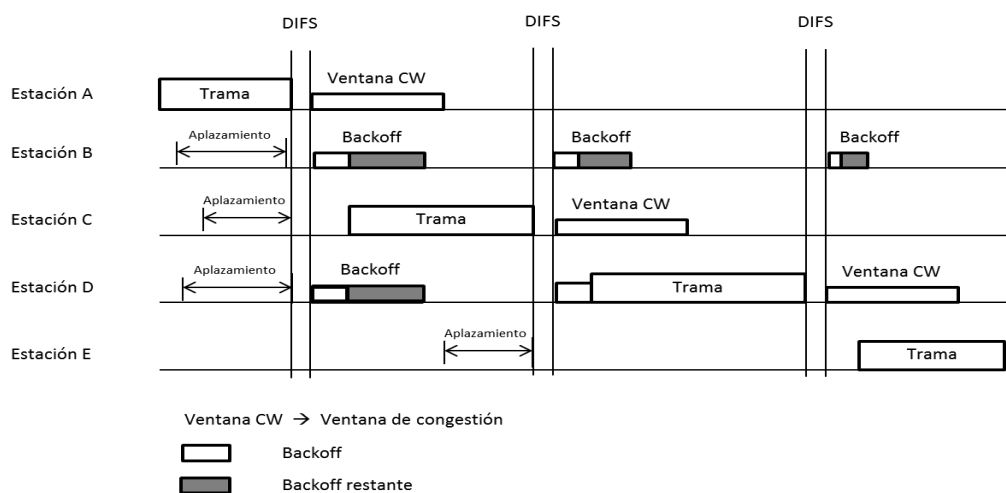


FIGURA 7 MECANISMO DE BACKOFF

Como se observa, al comenzar el procedimiento de backoff, la estación que ha registrado la colisión ajusta el contador de backoff en un valor numérico aleatorio.

Es importante recalcar que todos los slots de backoff se registran durante el tiempo DIFS, debido a que durante dicho periodo, la estación considera que el medio se encuentra idle y es cuando se produce una colisión por el acceso, dando como resultado dicha técnica de contienda.

La estación transmisora que está realizando el procedimiento de backoff debe a su vez emplear los mecanismos de sensado de portadora para continuar monitorizando el tráfico y si no encuentra actividad durante la duración de un slot de backoff, dicho mecanismo decrementa el contador.

Si por otra parte el medio se determina en su condición de *busy* durante el periodo de un slot, el mecanismo de backoff es suspendido y no realiza el decremento del contador.

El medio debe ser determinado en la condición idle durante el tiempo que estipula DIFS antes de que se permita que el procedimiento de backoff pueda continuar.

Tras dichas cláusulas, una vez que el contador de backoff llega a 0, la transmisión puede volver a comenzar.

El procedimiento de backoff debe ser llevado a cabo inmediatamente después de todas las transmisiones de una trama para cualquiera de los tipos definidos, control, gestión y datos, incluso si no existen tramas adicionales para ser enviadas.

En el caso de una transmisión que ha sido efectuada correctamente, este procedimiento de backoff debe ser iniciado al recibir la trama de confirmación por parte de la estación receptora.

Por otra parte, en el caso de que no exista confirmación por parte de la estación receptora que indique que la transmisión ha sido incorrecta, el mecanismo de backoff se iniciará cuando el timeout de ACK se consuma.

Se define una transmisión no exitosa, aquella en la cual la trama ACK no es recibida por la estación transmisora con la dirección del destinatario.

Si una transmisión es exitosa, el valor de la ventana de contención (CW) es decrementado hasta el mínimo CW_{min} antes de que el tiempo de backoff sea seleccionado. Como resultado de este procedimiento se deduce, que las tramas enviadas por una estación transmisora siempre van a estar separadas por al menos un intervalo de backoff.

Como efecto de este proceso, se deduce que cuando múltiples estaciones están compitiendo y seleccionando tiempos aleatorios de backoff, aquella estación que seleccione el tiempo menor empleando las funciones aleatorias será la que obtenga el canal para transmitir.

6.3. PROCEDIMIENTOS DE RECUPERACIÓN Y LÍMITES DE RETRANSMISIÓN.

Bajo el método de la DCF la responsabilidad de la recuperación frente a fallos en la transmisión recae en la estación transmisora que inicia la secuencia de intercambio de tramas.

Existen numerosa causas por las cuales se puede producir un fallo en la transmisión, por ejemplo, la trama CTS (clear to Send) puede que no sea devuelta por la estación transmisora tras la solicitud de las tramas RTS(Request to send), esto puede suceder debido a una colisión con tráfico de otras estaciones, interferencias en el canal o debido a que la estación que debe enviar la trama CTS está bajo condiciones de medio ocupado.

La recuperación frente a errores, realiza el proceso de retransmisión de las secuencias que durante el intercambio de tramas han sido fallidas. Este proceso se lleva a cabo por cada secuencia de tramas que ha sido defectuosa hasta que la transmisión ha sido realizada con éxito o hasta que se alcanzan los límites de tiempo en una retransmisión.

Las estaciones deben mantener un SRC (*Short retrycount*) y un LRC (*Largeretrycount*) para cada MSDU, ambos contadores son incrementados y decrementados independientemente uno del otro.

6.4. RELACIONES DE TIEMPO PARA LA DCF

Las relaciones temporales entre las especificaciones IFS se definen como gaps de tiempo en el medio.[3][7]

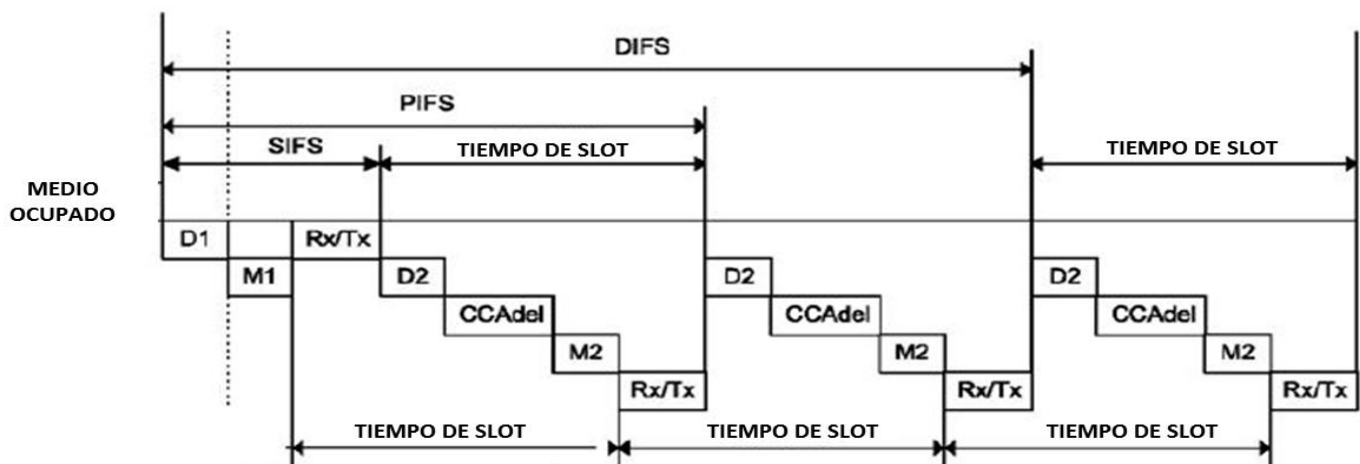
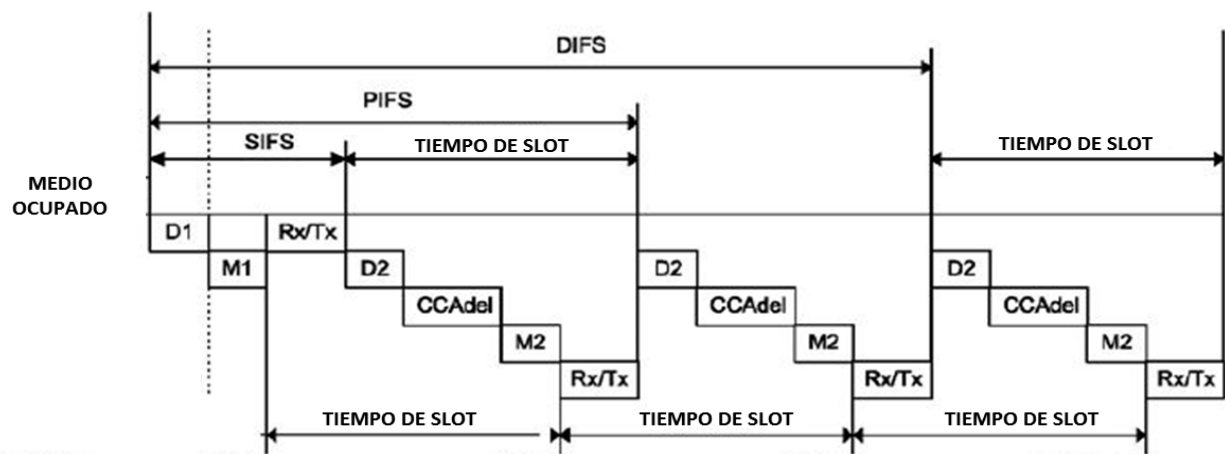


FIGURA 8 RELACIONES TEMPORALES

Todos los tiempos del medio inalámbrico hacen referencia al final de la transmisión y desde el final del último símbolo transmitido.

El comienzo de la transmisión está referido al primer símbolo de preámbulo de la siguiente unidad de datos a transmitir.

A continuación se definen los tiempos que influyen en el acceso al medio inalámbrico.



$D1 = aRxRfDelay + aRxPLCPDelay$
 $D2 = D1 + \text{Retardo por propagación en el aire}$
 $Rx / Tx = aRxTxTurnaroundTime$
 $M1 = M2 = aMACP \text{ Retardo de procesado}$
 $CCAdel = aCCA \text{ Tiempo} - D1$

FIGURA 9 DESCRIPCIÓN ELEMENTOS TEMPORALES

6.4.1. SLOT TIME

Como anteriormente ha sido definido, un slot time hace referencia al tiempo de slot en el cual el medio permanece libre de colisiones, se define como sigue:

$$\text{Slot time} = aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProceessiongDelay$$

El tiempo de slot tiene que ser compensado por los siguientes parámetros: [1]

- $aCCATime$: tiempo tomado por el receptor en realizar un asentimiento para indicar que el canal está libre.
- $RxTxTurnaroundTime$: tiempo de vuelta de indicación de canal del receptor al transmisor.
- $aAirPropagationTime$: retraso producido por el tiempo de propagación.
- $aMACProcessingDelay$: tiempo empleado por la capa MAC en completar el proceso.

6.4.2. INTERFRAME SPACING

De los diferentes espacios entre trama que especifica el estándar, tres son los empleados por la capa MAC para el acceso al medio.

El espacio entre tramas genera diferentes niveles de prioridad en función del tipo de paquetes. Los paquetes con un mayor grado, tienen un espacio entre tramas menor y por el contrario aquellos con menor prioridad accederán al canal más tarde.

6.4.2.1. SIFS (SHORT INTERFRAME SPACE)

El espacio entre tramas corto (SIFS) es empleado para los paquetes con un mayor grado de prioridad, tales como las tramas RTS/CTS y los ACK's.

Dicho espacio se define como sigue:

$$SIFS = aRXRFDelay + aRXPLCPDelay + aMACProcessingDelay + aRXTXTurnaroundTime$$

- *aRXRFDelay*: tiempo de retardo producido en el canal de RF del medio inalámbrico.
- *aRXPLCPDelay*: este retardo es causado por el preámbulo del PLCP (*physical layer convergence procedure*)
- *aMACProcessingDelay*: tiempo empleado por la capa MAC en completar el proceso.
- *RxTxTurnaroundTime*: tiempo de vuelta de indicación de canal del receptor al transmisor.

6.4.2.2. DCF INTERFRAME SPACE(DIFS)

Este espacio entre tramas se define como el mínimo tiempo necesario que el canal debe permanecer libre de colisiones (idle), antes de que los nodos de acceso aleatorio puedan acceder al canal.

Se define como sigue:

$$DIFS = SIFSTime + 2 \times SlotTime.$$

6.4.2.3. EXTENDED INTERFRAME SPACE (EIFS)

Este espacio no siempre dispone de un valor fijo de tiempo, se emplean en los casos que existe un error en la transmisión de paquetes.

6.5. CONCLUSIÓN ACCESO DCF

A continuación, se detalla a modo de conclusión general los aspectos más destacados de la capa MAC y el acceso bajo la función de distribución coordinada DCF empleando el protocolo CSMA.

6.5.1. REGLAS ESPECÍFICAS DEL ESTÁNDAR 802.11

El estándar 802.11 especifica un conjunto de reglas básicas que se emplean bajo todos los supuestos, algunas reglas más específicas se pueden aplicar en función del escenario y las circunstancias.[4][3]

1. Si mediante el sensado del canal, se detecta que el canal permanece en estado idle con una duración de tiempo mayor o igual que DIFS, la transmisión de ese nodo puede comenzar inmediatamente.
2. Si un paquete es recibido sin errores, el medio debe permanecer libre durante un intervalo de tiempo como mínimo DIFS antes de que pueda comenzar otra transmisión.
3. Una vez que una estación envíe satisfactoriamente el primer paquete de una secuencia, dicha estación tiene el control del canal.

4. El nodo transmisor debe ser el encargado de gestionar la detección de errores y las retransmisiones.
5. Se debe enviar un asentimiento (ACK) por parte del receptor para todas las tramas de datos que son enviadas y recibidas.
6. Para que una transmisión sea exitosa, deben cumplirse todos los requisitos, como el correcto intercambio sin errores de las tramas RTS/CTS y los ACK. En el caso de que exista algún error, debe ser realizado de nuevo el proceso.

6.5.2. REGLAS ESPECÍFICAS DE LA DCF

Como se ha comentado anteriormente, el método de acceso gestionado por la capa MAC que nos interesa en este trabajo es el de la DCF que opera bajo el protocolo CSMA.[3][4]

A continuación se definen un conjunto de reglas específicas de este modo de acceso.

1. El sensado del canal se realiza mediante mecanismos físicos y virtuales.
2. Si la transmisión es llevada a cabo con errores , el canal debe permanecer en estado idle durante el tiempo EIFS.
3. Si el medio es sensado y se detecta ocupado, la estación transmisora debe esperar hasta que el canal vuelva a estar libre.
4. Cualquier fallo en un paquete, incrementa el *retrycounter*.

5. Cualquier paquete que sea enviado una vez superado el umbral que define la trama RTS, será descartado, debiendo existir un nuevo intercambio de tramas entre emisor y receptor RTS/CTS.
6. El *retrycounter* es puesto a cero solo en el caso de que se reciba la trama CTS por parte del receptor.

6.6. MODELO TEÓRICO DE LA DCF

A continuación, se muestra la descripción del modelo teórico empleado para el cálculo de la eficiencia del protocolo CSMA.

Emplearemos los resultados teóricos para compararlos con las simulaciones y obtener una predicción del rendimiento de la red empleando el estándar 802.11.

Para realizar el estudio teórico se empleará el modelo de Bianchi, el cual fue realizado por Giuseppe Bianchi, y que permite modelar de forma analítica el estándar 802.11 basado en el protocolo de la DCF.[8]

Dicho estudio fue concebido para determinar la saturación del throughput en una red inalámbrica, permitiendo calcular la probabilidad de que exista una colisión en la transmisión de paquetes.

El modelo de Bianchi [8] emplea una cadena de Markov con $m + 1$ etapas de Backoff, donde cada etapa representa un incremento del contador de *backoff* debido a la colisión de paquetes enviados por nodos distintos, procediendo así al incremento de forma exponencial de la ventana de contención (C_w).

6.6.1. CADENA DE MARKOV

A continuación se presenta el modelo de cadena Bianchi – Markov empleado para la representación analítica del protocolo CSMA.[8]

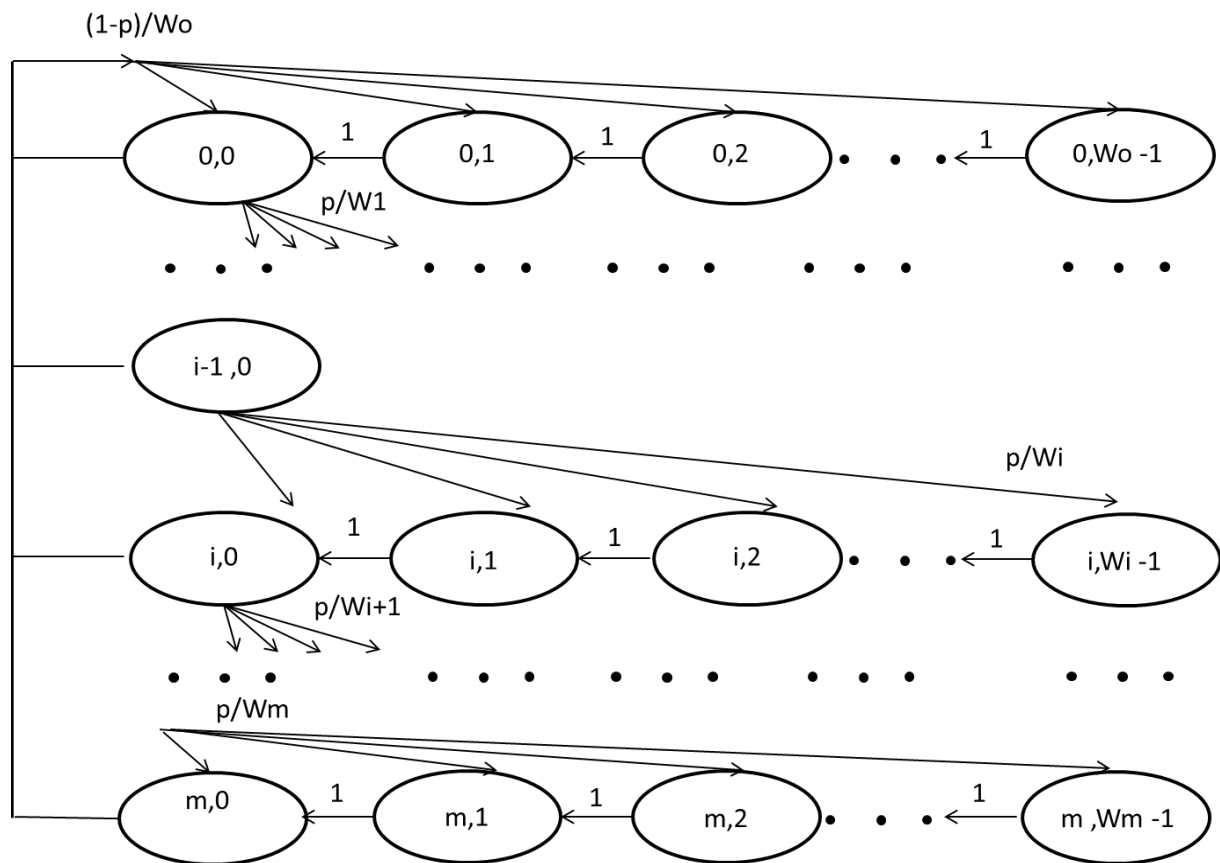


FIGURA 10 CADENA DE BIANCHI-MARKOV

- W : es el mínimo valor de la ventana de contención.
- N : número de estaciones (STA)
- M : es el máximo valor del contador de Backoff
- W_i : es el valor de la ventana de contención para un valor i de Backoff
- P : es el valor de la probabilidad de colisión para un paquete.

En cada etapa de la cadena de Bianchi – Markov , el valor de W_i es el máximo valor de la ventana de contención y es igual a $2^m(CW_{min}+1)$.

Si se produce una transmisión correcta en el estado $(i,0)$, se escoge un valor aleatorio de Backoff comprendido entre los valores 0 y (CW_0-1) , como se describe en 802.11 IEEE [3].

En el caso de que exista una colisión, se selecciona un valor aleatorio de backoff comprendido entre los valores 0 y (CW_i-1) . Este caso viene representado por los estados comprendidos entre $(i,0)$ a $(i, W_i -1)$.

Este modelo adopta una escala discreta de tiempo, donde cada estado es representado por $\{s(t), b(t)\}$, donde $b(t)$ es el proceso estocástico que representa el contador de backoff para una estación transmisora y $s(t)$ es el proceso estocástico que representa la etapa del contador de backoff $(0,1,2...m)$ para una estación transmisora en un instante de tiempo determinado.

Derivado de las explicaciones anteriores, se detallan las fórmulas que definen analíticamente la cadena de Bianchi – Markov.

Expresiones analíticas:

Se define la probabilidad de colisión de un paquete, debido a la transmisión de una estación, en el intervalo de tiempo *slot time* , como **p** .

Se define la variable **π** como la probabilidad de que otra estación inicie una transmisión durante el mismo slot time que otra estación.

La probabilidad de colisión queda determinada por:

$$p = 1 - (1 - \pi)N - 1$$

La probabilidad de que una estación transmisora envíe un paquete durante el periodo de *time slot* se indica como sigue[8]

$$\sum_{i=0}^m b(i, 0) = \frac{b(0,0)}{1-p} = \frac{2(1-2p)}{(1-2p)(Wmin+1) + pWmin(1-(2p)^m)}$$

Quedando resumida en la siguiente expresión:

$$\sum_{i=0}^m b_{i,0} = \frac{2}{1 + Wmin + pWmin \sum_{k=0}^{m-1} (2p)^k}$$

Una vez que se obtienen las probabilidades de transmisión de paquetes por parte de una estación y la probabilidad de colisión de paquetes, se puede obtener el throughput de la red, como relación entre los datos de *payload* transmitidos y el tiempo de slot.[8]

$$Throughput = \frac{E [\text{información de payload por cada time slot}]}{E[\text{duración del time slot}]}$$

De las anteriores formulas, se define en el documento de Giuseppe Bianchi la solución numérica para el througput de las estaciones que acceden al medio en función del número de estaciones en el canal.

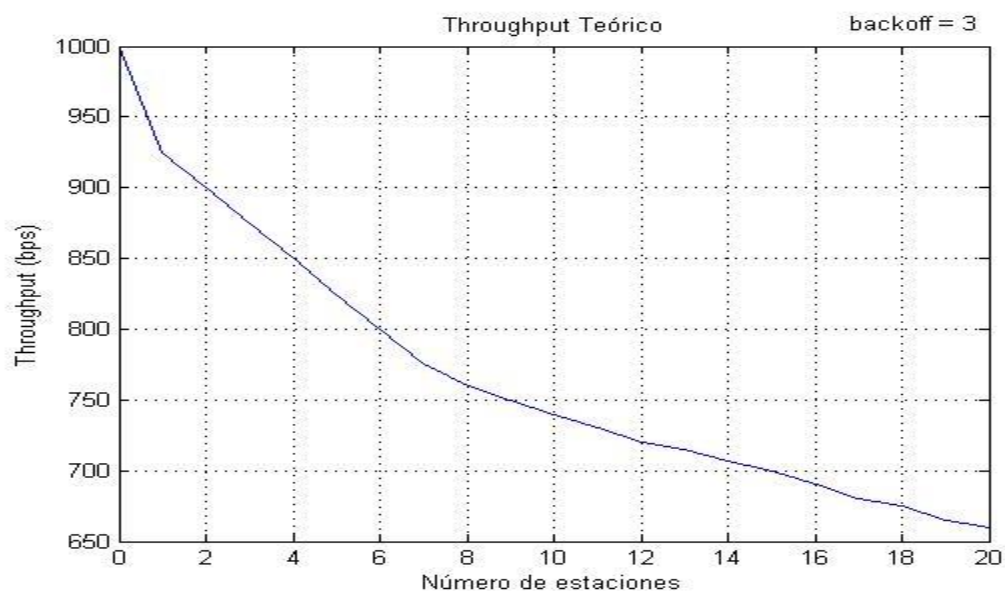


FIGURA 11 THROUGHPUT TEÓRICO

7. SIMULACIÓN DE ESTÁNDAR WIFI 802.11

Una vez estudiados los parámetros que rigen el acceso para la tecnología inalámbrica WIFI, procederemos a realizar una simulación del estándar, reproduciendo su modelo matemático.

7.1. SIMULADOR NS2

El simulador *Networ Simulator 2* es un software que permite realizar la simulación de eventos discretos, creado y difundido para la investigación en redes telemáticas. [9][10]

Proporciona soporte para la simulación de muchos protocolos de las capas de aplicación o transporte.

Permite la simulación de redes tanto cableadas como inalámbricas y el uso de topologías complejas con diversos tipos de tráfico.

En el caso de estudio que nos ocupa, es empleado para los mecanismos que hacen referencia a la capa de **enlace de datos** en redes inalámbricas, como MAC (Medium Access Control) y el mecanismo de acceso al medio CSMA.

A continuación se ilustran los escenarios de una red realista frente a la gestión que realiza NS2

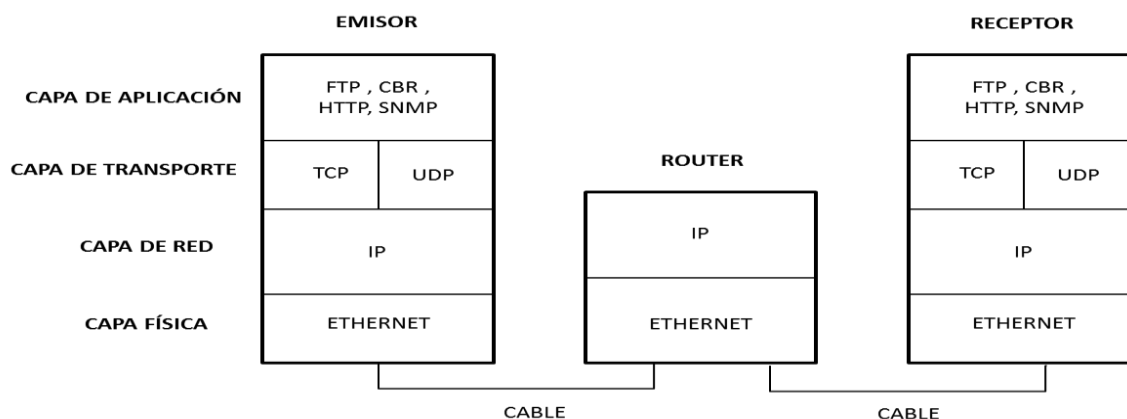


FIGURA 12 MODELO SIMULADOR NS2

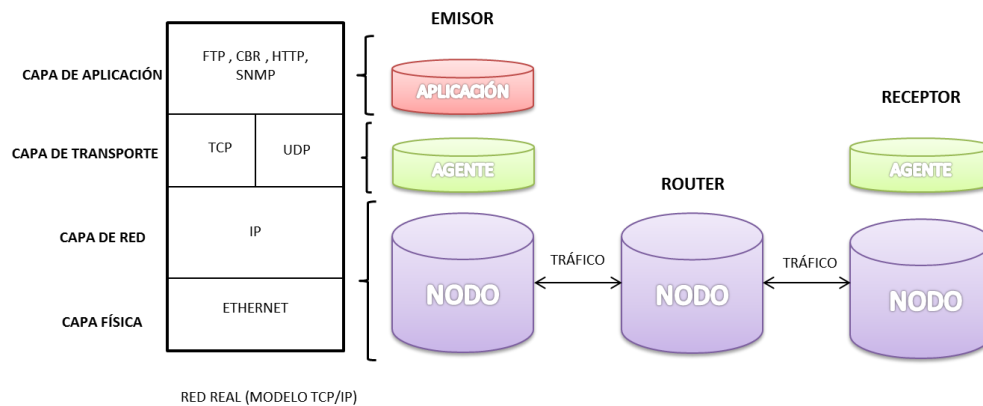


FIGURA 13 MODELO SIMULADOR NS2

El software NS2 se define como un simulador orientado a objetos, definido mediante el lenguaje **C++**.

La interfaz de usuario permite realizar la definición de los elementos que serán simulados (Nodos, tipo de enlace, tipo de tráfico, etc) mediante el lenguaje **TCL**.

Los scripts generados por la aplicación se basan en librerías definidas en módulos del propio simulador, en las cuales se definen múltiples sistemas de comunicación.

En el caso que nos ocupa, las librerías empleadas son las del estándar WIFI 802.11 que define la capa de acceso (MAC) así como los mecanismos de detección de colisiones y el estado del canal inalámbrico.

En el script TCL generado, se hace uso de esta librerías para definir y modificar los parámetros que definen el estándar, como el tamaño de la ventana de contención (Cw) el intervalo de time slot para la transmisión, la velocidad básica del enlace y los espacios entre tramas SIFS.

7.2. INSTALACIÓN DEL SIMULADOR

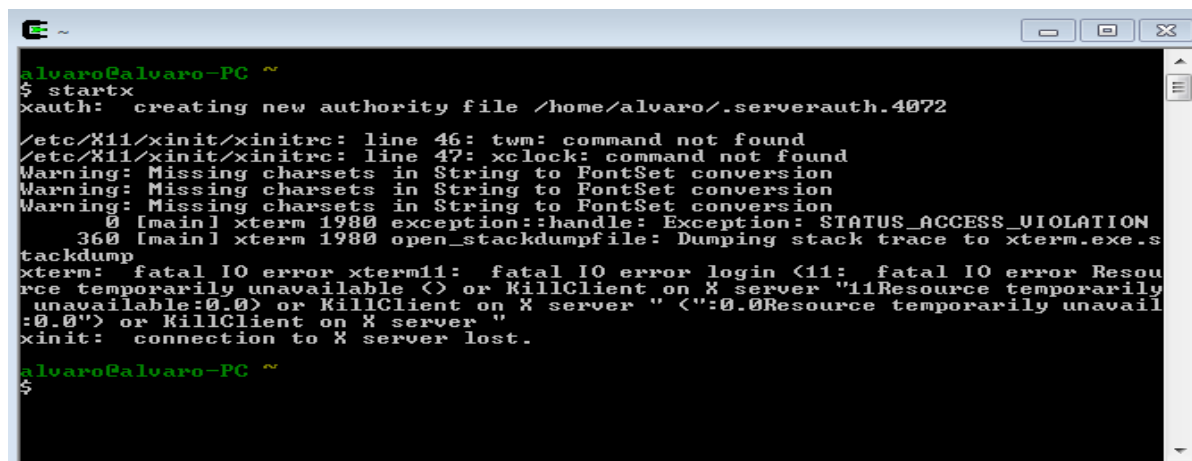
A continuación se detalla la instalación del software de simulación NS2 bajo la plataforma de trabajo elegida, que será Windows 7.[11][9]

Inicialmente el programa NS2 ha sido desarrollado para el sistema operativo Linux, pero por comodidad se empleará una máquina virtual llamada Cywin que simula dicho S.O.

La descarga de los ficheros se realiza directamente de la página de ISI <http://www.isi.edu/nsnam/ns/> donde accedemos a toda la documentación y archivos necesarios.

Por otra parte procedemos a descargar e instalar la máquina virtual Cygwin y la versión más reciente de Active TCL (8.4.7).

Tras crear el directorio de trabajo en C:/ns, iniciamos la máquina virtual Cygwin mediante el comando "startx",



```
alvaro@alvaro-PC ~  
$ startx  
xauth: creating new authority file /home/alvaro/.serverauth.4072  
/etc/X11/xinit/xinitrc: line 46: twm: command not found  
/etc/X11/xinit/xinitrc: line 47: xclock: command not found  
Warning: Missing charsets in String to FontSet conversion  
Warning: Missing charsets in String to FontSet conversion  
Warning: Missing charsets in String to FontSet conversion  
[main] xterm 1980 exception::handle: Exception: STATUS_ACCESS_VIOLATION  
360 [main] xterm 1980 open_stackdumpfile: Dumping stack trace to xterm.exe.s  
tackdump  
xterm: fatal IO error xterm11: fatal IO error login <11: fatal IO error Resou  
rce temporarily unavailable <> or KillClient on X server "11Resource temporarily  
unavailable:0.0) or KillClient on X server " <":0.0Resource temporarily unavail  
:0.0") or KillClient on X server "  
xinit: connection to X server lost.  
alvaro@alvaro-PC ~  
$
```

FIGURA 14 MÁQUINA VIRTUAL

Tras este procedimiento, ya disponemos del entorno Linux que permite correr el software NS2.

Iniciando el siguiente terminal de comandos invocamos al software mediante "ns" disponiendo así acceso a todas sus funciones.

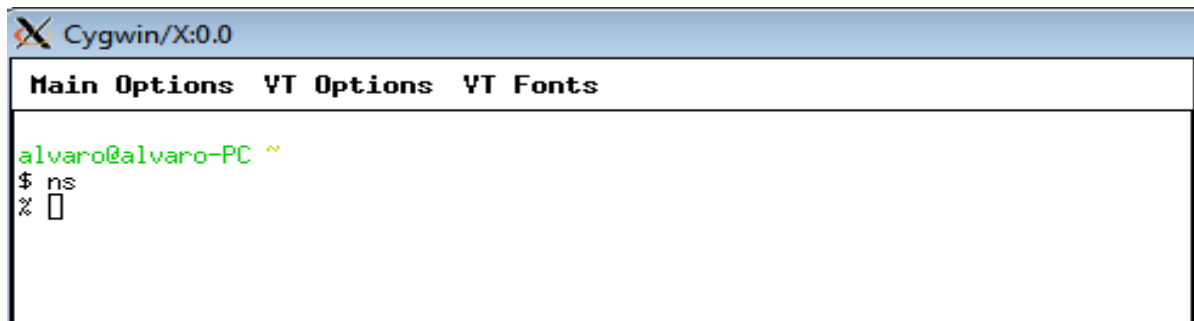


FIGURA 15 EJECUTAR SIMULADOR

7.3. APLICACIONES ADICIONALES

Dispone de herramientas para mostrar los resultados en forma gráfica como nam y Tracegraph los cuales permiten ver la topología y los resultados de la simulación.

- **NAM** [9][11]

Mediante este software adicional al simulador NS2 podemos visualizar la topología de la red creada y a su vez iniciar visualmente la simulación, viendo el intercambio de paquetes , el envío de tramas RTS/CTS y los ACK de confirmación.

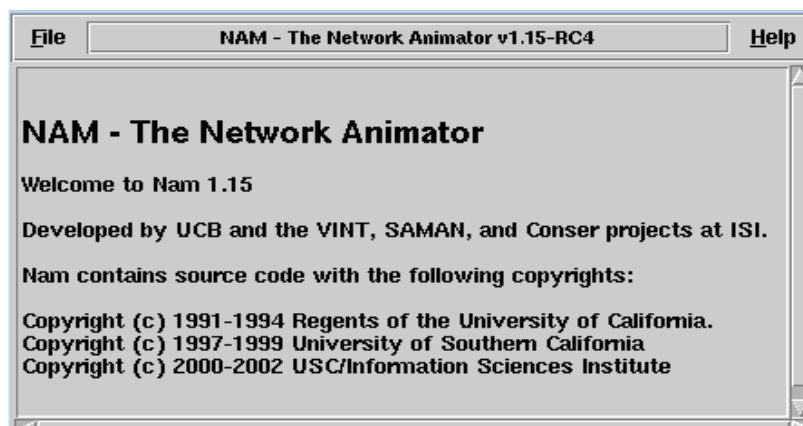


FIGURA 16 NAM

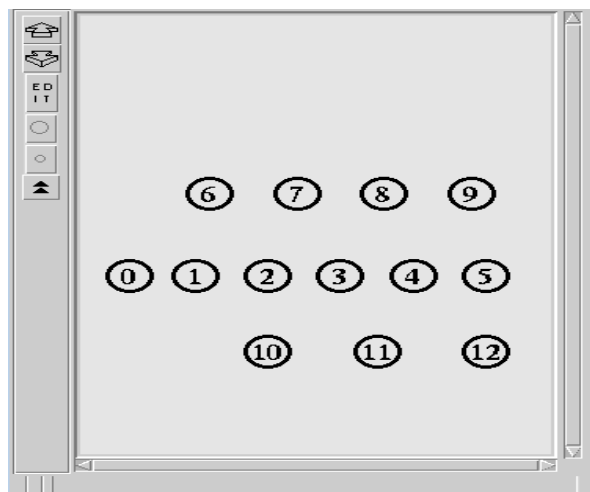


FIGURA 17 TOPOLOGÍA DE RED

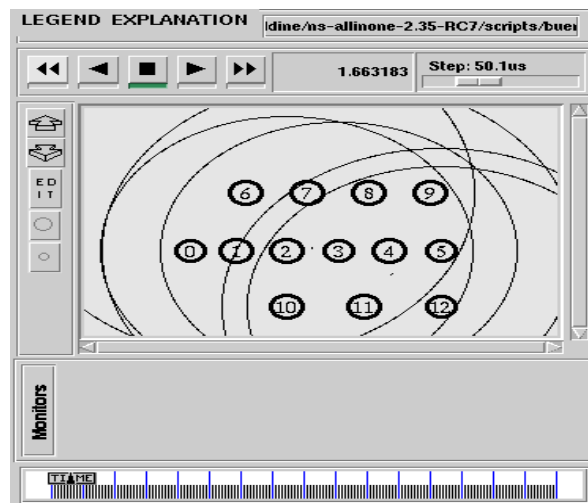


FIGURA 18 TRÁFICO GENERADO

En las imágenes anteriores podemos observar la disposición de la topología de la red creada que consta de 13 nodos de tipo inalámbrico, distribuidos en una cuadrícula de dimensiones prefijadas.

En la figura observamos como los nodos realizan el protocolo de encaminamiento y routing mediante el intercambio de tramas para descubrir nodos vecinos.

En la siguiente figura, una vez fijadas las rutas por todos los nodos, vemos el intercambio de paquetes.

En este instante se aprecia un paquete con origen el nodo 3 y destino el nodo 6.

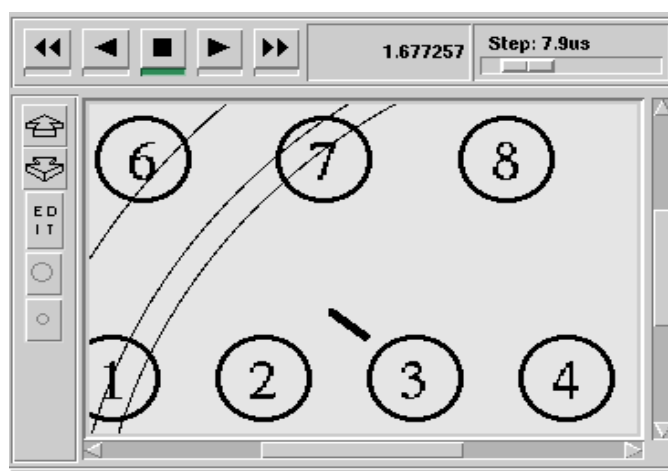


FIGURA 19 TRÁFICO GENERADO 2

- **Tracegraph.[9][11]**

El software de simulación NS2, no permite por si solo mostrar los resultados generados, genera ficheros de texto denominados “trazas”, los cuales serán interpretados por la herramienta *tracegraph* para seleccionar el tipo de mensaje que se desea monitorar (tramas RTS/CTS , paquetes TCP o ACK's).

A continuación se detalla el formato del archivo traza generado por el simulador para la topología mostrada anteriormente.

```

10131 s 8.211541422 _7_ MAC --- 0 RTS 44 [62e 4 7 0]
10132 r 8.211893799 _4_ MAC --- 0 RTS 44 [62e 4 7 0]
10133 s 8.211903799 _4_ MAC --- 0 CTS 38 [4f4 7 0 0]
10134 r 8.212208176 _7_ MAC --- 0 CTS 38 [4f4 7 0 0]
10135 s 8.212218176 _7_ MAC --- 883 ack 118 [13a 4 7 800] ----- [7:1 4:0 32 4] [29 0] 0 0
10136 r 8.213162553 _4_ MAC --- 883 ack 60 [13a 4 7 800] ----- [7:1 4:0 32 4] [29 0] 1 0
10137 s 8.213172553 _4_ MAC --- 0 ACK 38 [0 7 0 0]
10138 r 8.213476930 _7_ MAC --- 0 ACK 38 [0 7 0 0]
10139 s 8.213546720 _3_ MAC --- 0 RTS 44 [62e 6 3 0]
10140 s 8.213546851 _9_ MAC --- 0 RTS 44 [256e c 9 0]
10141 s 8.213546853 _12_ MAC --- 0 RTS 44 [62e 9 c 0]
10142 D 8.213547451 _6_ MAC COL 0 RTS 44 [62e 6 3 0]
10143 s 8.214333369 _12_ MAC --- 0 RTS 44 [62e 9 c 0]
10144 r 8.214685887 _9_ MAC --- 0 RTS 44 [62e 9 c 0]
10145 s 8.214695887 _9_ MAC --- 0 CTS 38 [4f4 c 0 0]
10146 r 8.215000404 _12_ MAC --- 0 CTS 38 [4f4 c 0 0]
10147 s 8.215010404 _12_ MAC --- 1089 ack 118 [13a 9 c 800] ----- [12:0 9:0 32 9] [59 0] 0 0
10148 r 8.215954922 _9_ MAC --- 1089 ack 60 [13a 9 c 800] ----- [12:0 9:0 32 9] [59 0] 1 0
10149 s 8.215964922 _9_ MAC --- 0 ACK 38 [0 c 0 0]
10150 r 8.216269440 _12_ MAC --- 0 ACK 38 [0 c 0 0]
10151 s 8.216359322 _7_ MAC --- 0 RTS 44 [62e 4 7 0]
10152 r 8.216711699 _4_ MAC --- 0 RTS 44 [62e 4 7 0]
10153 s 8.216721699 _4_ MAC --- 0 CTS 38 [4f4 7 0 0]
10154 r 8.217026076 _7_ MAC --- 0 CTS 38 [4f4 7 0 0]
10155 s 8.217036076 _7_ MAC --- 889 ack 118 [13a 4 7 800] ----- [7:1 4:0 32 4] [30 0] 0 0
10156 r 8.217980453 _4_ MAC --- 889 ack 60 [13a 4 7 800] ----- [7:1 4:0 32 4] [30 0] 1 0
10157 s 8.217990453 _4_ MAC --- 0 ACK 38 [0 7 0 0]
10158 r 8.218294831 _7_ MAC --- 0 ACK 38 [0 7 0 0]
10159 s 8.218404453 _4_ MAC --- 0 RTS 44 [256e 7 4 0]
10160 r 8.218756831 _7_ MAC --- 0 RTS 44 [256e 7 4 0]
10161 s 8.218766831 _7_ MAC --- 0 CTS 38 [2434 4 0 0]
10162 r 8.219071208 _4_ MAC --- 0 CTS 38 [2434 4 0 0]
10163 s 8.219081208 _4_ MAC --- 1197 tcp 1118 [13a 7 4 800] ----- [4:0 7:1 32 7] [30 0] 0 0
10164 r 8.228025585 _7_ MAC --- 1197 tcp 1060 [13a 7 4 800] ----- [4:0 7:1 32 7] [30 0] 1 0
10165 s 8.228035585 _7_ MAC --- 0 ACK 38 [0 4 0 0]
10166 r 8.228339962 _4_ MAC --- 0 ACK 38 [0 4 0 0]
10167 s 8.228429585 _7_ MAC --- 0 RTS 44 [62e 4 7 0]
10168 s 8.228429939 _1_ MAC --- 0 RTS 44 [62e a 1 0]
10169 D 8.228430439 _4_ MAC COL 0 RTS 44 [62e 4 7 0]
10170 D 8.228782240 _10_ MAC COL 0 RTS 44 [62e a 1 0]

```

FIGURA 20 ARCHIVO TRAZA

Podemos apreciar, como el archivo generado por el simulador se agrupa en columnas, registrando los eventos sucedidos en cada instante de tiempo.

Las columnas empleadas por la herramienta de visualización Tracegraph corresponden a las 8 primeras que se detallan a continuación:

1. Tipo de evento: “s” mensaje enviado, “r” mensaje recibido, “D” mensaje descartado por el receptor.
2. Marca temporal: corresponde al instante de tiempo del evento asociado.
3. Nodo emisor del mensaje: corresponde al nodo que envía el mensaje.
4. Nivel : corresponde al nivel MAC.
5. Colisión: indica si el paquete ha colisionado durante su envío. Aplicando las técnicas de contienda CSMA/CD.
6. ID : corresponde al identificador del paquete enviado.
7. Tipo de tráfico: TCP, ACK o RTS/CTS.
8. Tamaño del paquete (bits).

Una vez definidos los campos de interés, dicha herramienta se resume en los siguientes campos:

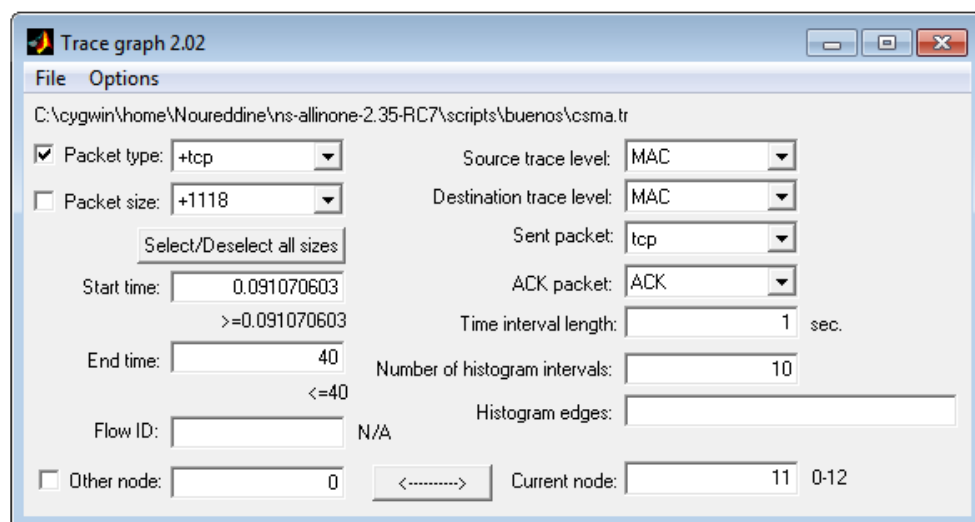


FIGURA 21 HERRAMIENTA TRACEGRAPH

Permite filtrar el tipo de paquete y la longitud del mismo, definiendo el nivel de la capa para el nodo emisor (MAC) y destino.

El resumen de la información de la simulación se muestra a continuación, donde nos informa del estado de la red ,así como de los paquetes enviados, recibidos y descartados.

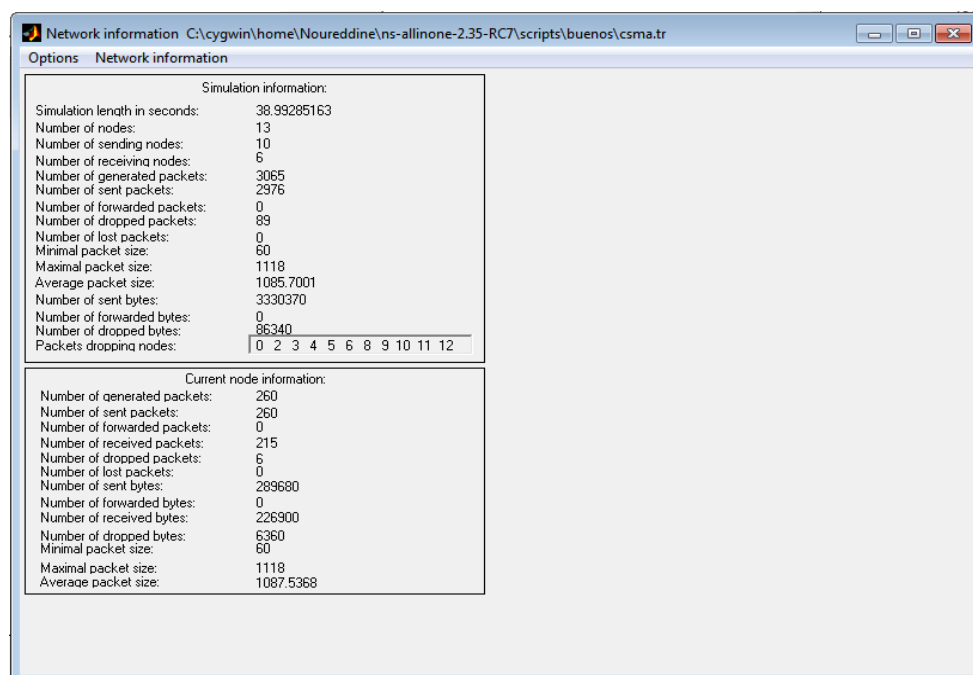


FIGURA 22 RESUMEN DE RED SIMULADA

7.4. PARÁMETROS DE LA SIMULACIÓN

A continuación se muestran los parámetros para la simulación base del estándar 802.11 mediante el protocolo de la DCF.[3][4][5][7]

Cwminima	15	-----
Cw máxima	1024	-----
Tiempo de Slot	20	microsegundos
Tamaño del buffer de recepción	50	paquetes
Longitud de paquete	1440	bits
Longitud de cabeceras	192	bits
Tasa de transmisión	1.0	Mbps
Short Retry Limit MAC	4	-----
Long Retry Limit MAC	7	-----
Short InterframeSpace	10	microsegundos

TABLA 2 PARÁMETROS DE SIMULACIÓN

El estudio que se llevará a cabo de las simulaciones, incluyen los siguientes apartados:

- Numero de colisiones en el acceso al medio variando los parámetros de la ventana de contención.
- Variación del parámetro Slot Time
- Variación del número de estaciones que acceden al medio.
- Variando el parámetro SIFS.

Los resultados bajo estudio que se detallarán a continuación son

- Throughput y goodputdel enlace.
- Número de paquetes descartados por los nodos.

8. SIMULACIONES DE LA DCF

En este apartado se analizan los aspectos más relevantes que definen las prestaciones de un sistema inalámbrico basado en el estándar 802.11 y el protocolo de acceso al medio CSMA.

El estudio consta de la simulación de los parámetros que define el estándar comparado con la modificación de los mismos para evaluar sus prestaciones.

8.1. VENTANA DE CONTENCIÓN

Como se ha descrito anteriormente, la ventana de contención dispone de un valor mínimo que define el estándar, fijado en 15. Dicho valor crece exponencialmente en el caso de que ocurran colisiones hasta alcanzar un valor superior (CW_{\max}) definido en 1024.

$$CW_{\min} = 15 \quad CW_{\max} = 1024$$

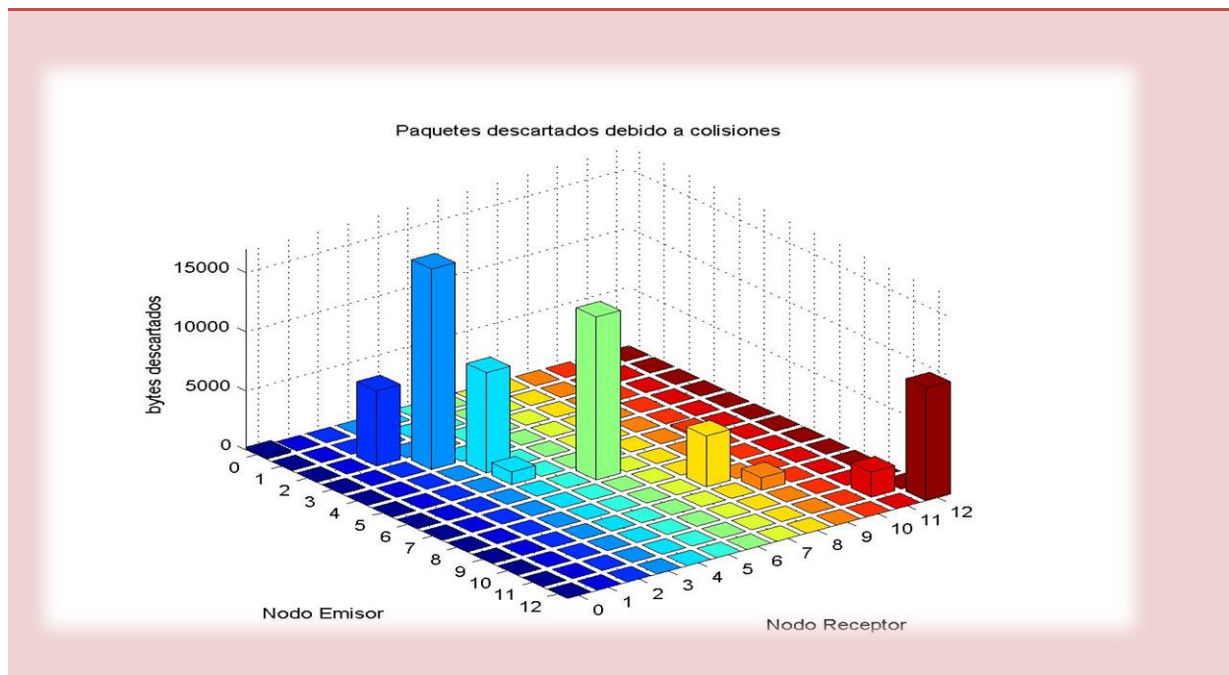


FIGURA 23 DESCARTE DE PAQUETES 1

En la figura 23 podemos observar el descarte de paquetes debido a las colisiones que se han producido en la red simulada.

Los parámetros de ventana de congestión empleados, son en este caso los definidos por el estándar 802.11 [3][6].

El eje vertical, hace referencia a los bytes descartados por la red, durante el tiempo que dura la simulación.

Los ejes horizontales hacen referencia a los nodos implicados en la transmisión de datos, enfrentando ambos ejes con los nodos emisores y con los nodos receptores.

El principal objetivo de ésta comparativa es observar la influencia del valor de la ventana de congestión teniendo como referencia los resultados obtenidos con la configuración que define el estándar 802.11.

$$CW_{min} = 15 \quad CW_{max} = 3000$$

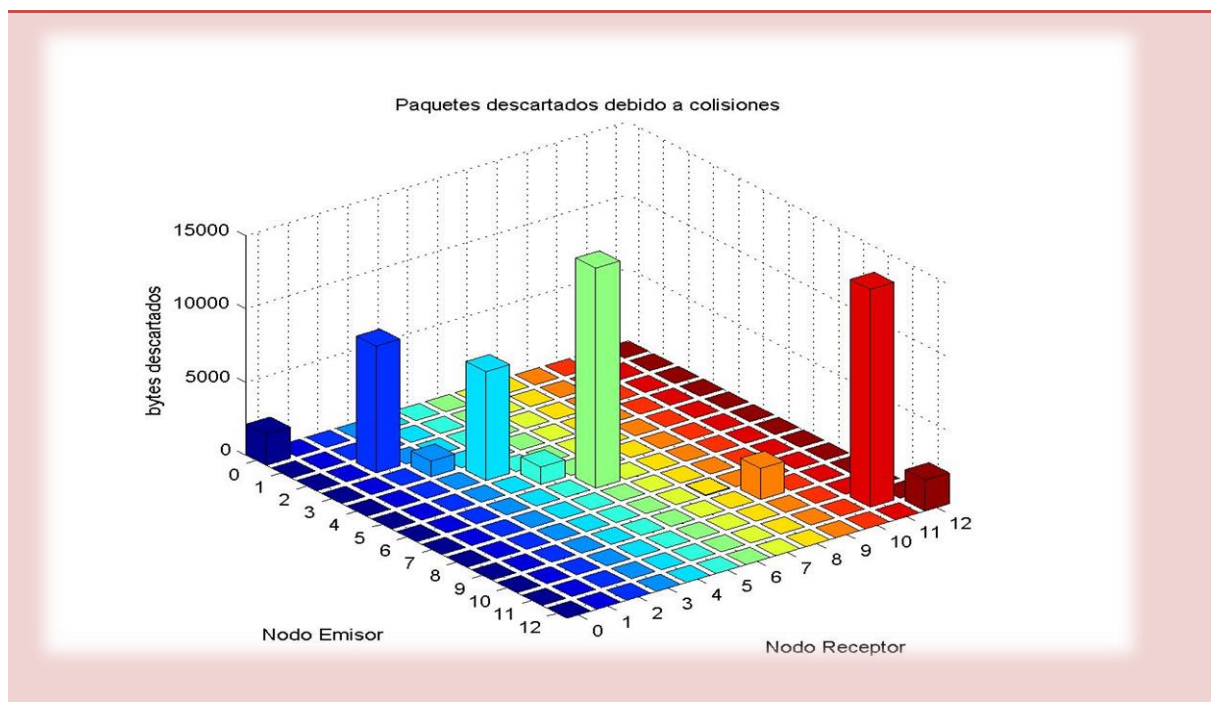


FIGURA 24 DESCARTE DE PAQUETES 2

En la figura 24, podemos observar la evolución del descarte de paquetes de la red simulada, variando el parámetro del valor superior de la ventana de congestión (CW_{max}).

Los resultados obtenidos, son muy similares en cuanto a tasa de descarte de paquetes con respecto a los proporcionados por la simulación con los parámetros definidos en 802.11.

Se puede extraer como conclusión, que el valor inferior de la ventana de congestión (CW_{min}) es el que determina el número de colisiones de la red.

Habiendo aumentado hasta 3000 unidades el valor superior, vemos cómo no existe una diferencia sustancial en los resultados, ya que el valor de la ventana de congestión aumenta exponencialmente, partiendo de su valor inferior una vez que ha ocurrido una colisión.

$$CW_{min} = 400 \quad CW_{max} = 1024$$

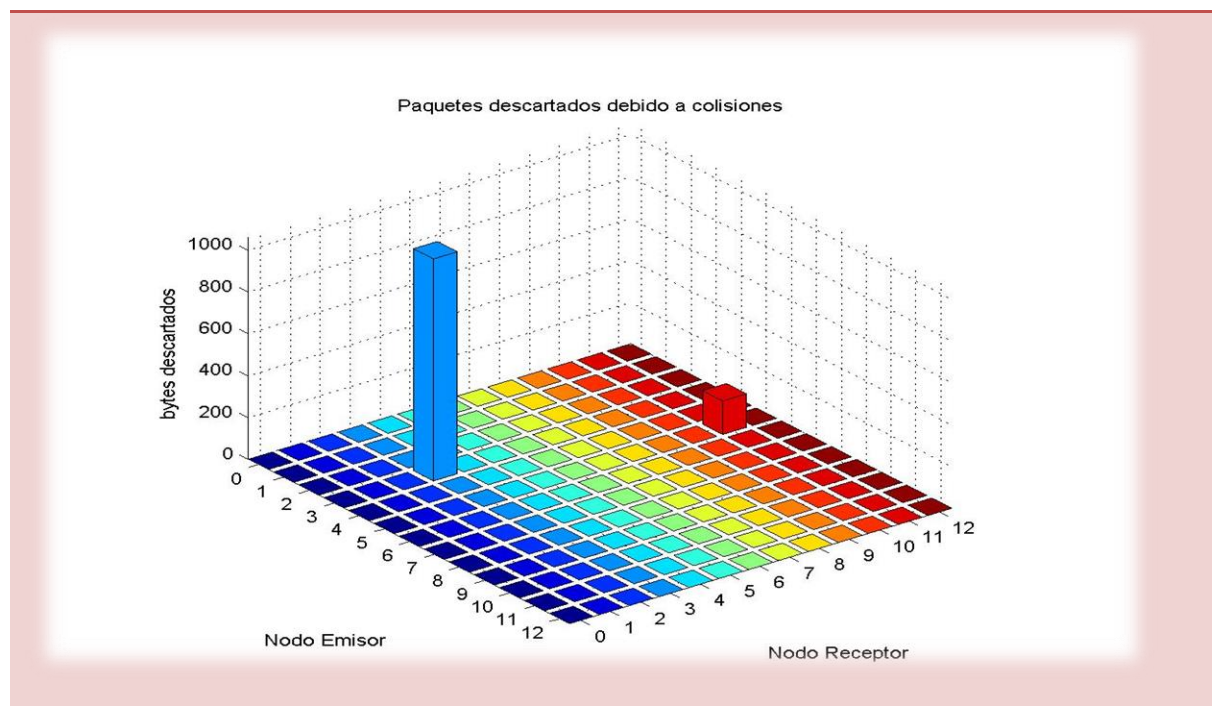


FIGURA 25 DESCARTE DE PAQUETES 3

En la figura 25, en la configuración de la ventana de congestión, se han establecido su parámetros CW_{min} en un valor elevado, (400) determinando así, el tiempo inicial que una estación transmisora debe esperar hasta poder volver a intentar la retransmisión del paquete colisionado.

Como consecuencia de un valor inicial elevado de la ventana de congestión, existirán muchos menos intentos de retransmisión de paquetes y por ello un menor número de colisiones.

A cambio de dicho beneficio, el throughput efectivo de cada estación transmisora, será muy bajo, debido a que el tiempo que permanece inactiva o en espera de retransmisión es muy elevado.

Otra consecuencia de dicho caso, es que al existir un tiempo de espera alto, existirán un número de estaciones que no puedan apenas transmitir sus datos debido a la probabilidad de encontrar el medio ocupado.

$$CW_{min} = 2 \quad CW_{max} = 200$$

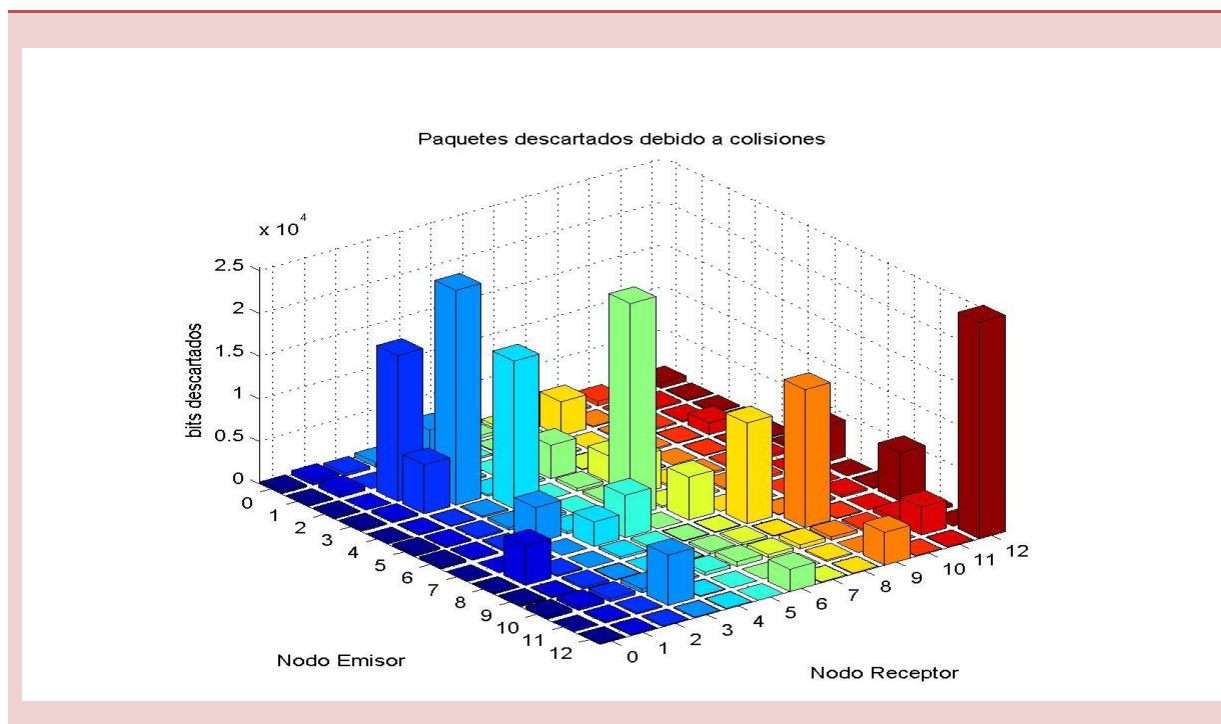


FIGURA 26 DESCARTE DE PAQUETES 4

En la figura 26, se realiza el estudio del descarte de paquetes, variando los valores superior e inferior de la ventana de congestión (CW_{min} y CW_{max}).

En éste caso, el valor inferior es de 2 unidades y el superior de 200 unidades.

Como consecuencia de éstas modificaciones, al establecer un valor inferior muy bajo, existirán un mayor número de colisiones iniciales debido al tiempo que la estación transmisora permanece a la espera de volver a intentar la transmisión del paquete.

En el caso del valor superior de la ventana de congestión, un valor sustancialmente más bajo del que determina el estándar 802.11, implica que si la red está saturada en un instante determinado, aquellas estaciones que están provocando colisiones de paquetes, no esperen el tiempo necesario para volver a realizar la retransmisión, produciendo más colisiones.

A continuación se describirán los resultados anteriores, en forma de gráfica 2-D, donde se puede observar la evolución del descarte de paquetes de la red simulada en función del tiempo de la simulación.

En los casos siguientes, las gráficas quedan representadas por los siguientes conceptos.

- Eje de ordenadas: evolución temporal de la simulación.
- Eje de abscisas: evolución de los bytes descartados en un instante determinado.

$$CW_{min} = 15 \quad CW_{max} = 1024$$

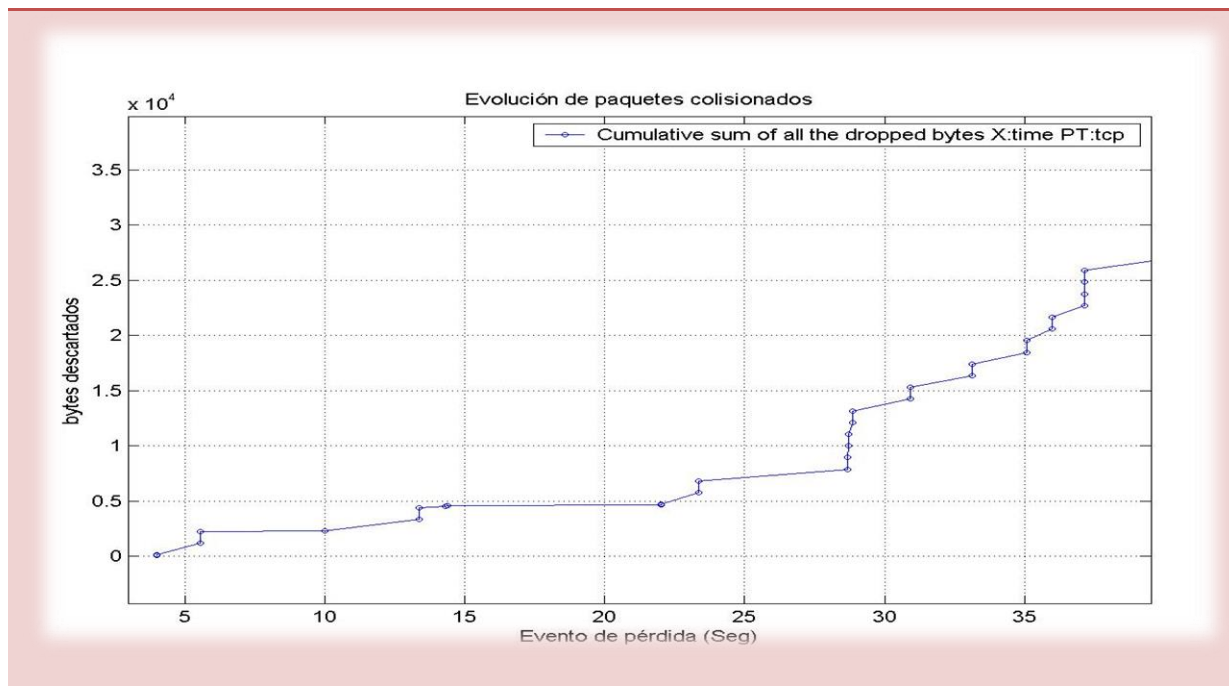


FIGURA 27 EVOLUCIÓN TEMPORAL 1

$CW_{min} = 15$ $CW_{max} = 3000$

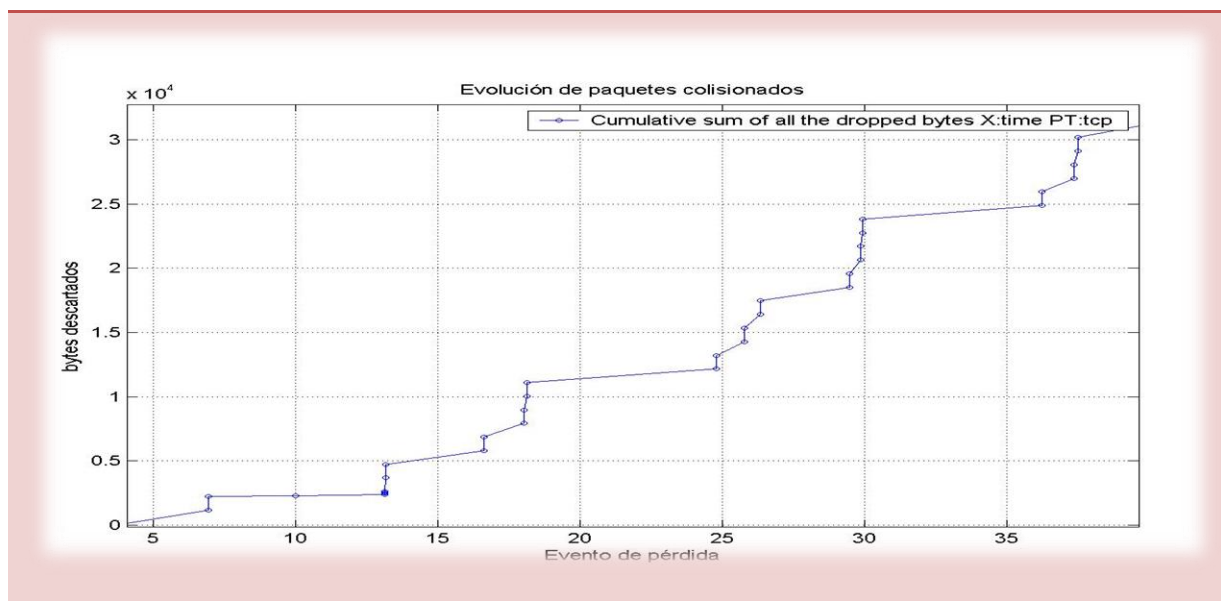


FIGURA 28 EVOLUCIÓN TEMPORAL 2

$CW_{min} = 400$ $CW_{max} = 1024$

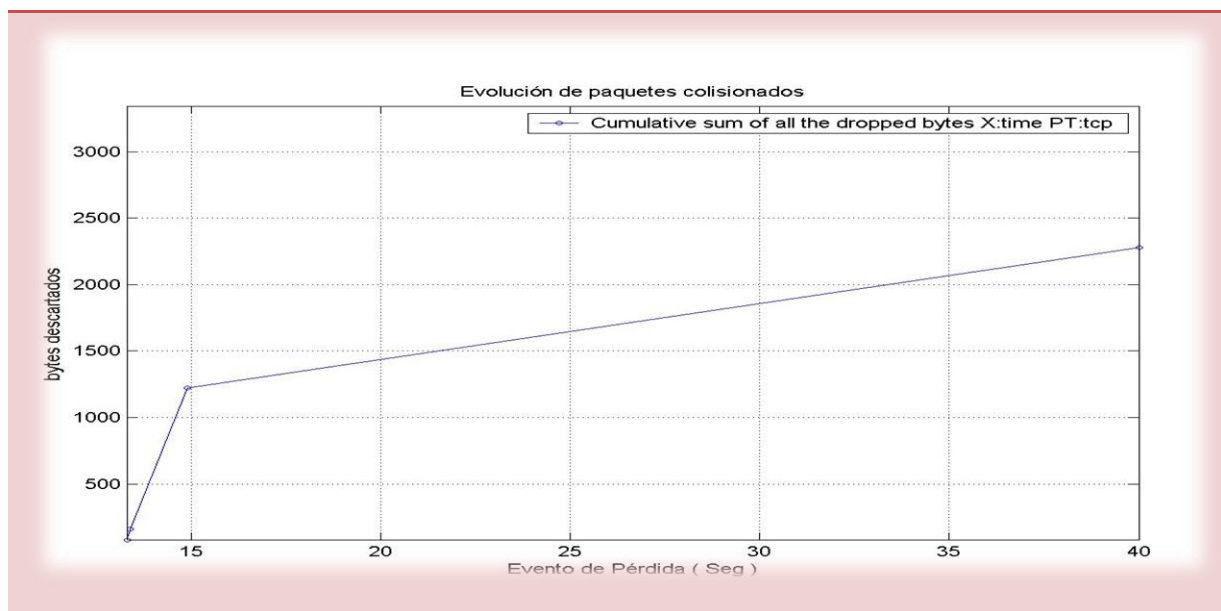


FIGURA 29 EVOLUCIÓN TEMPORAL 3

$CW_{min} = 2$ $CW_{max} = 200$

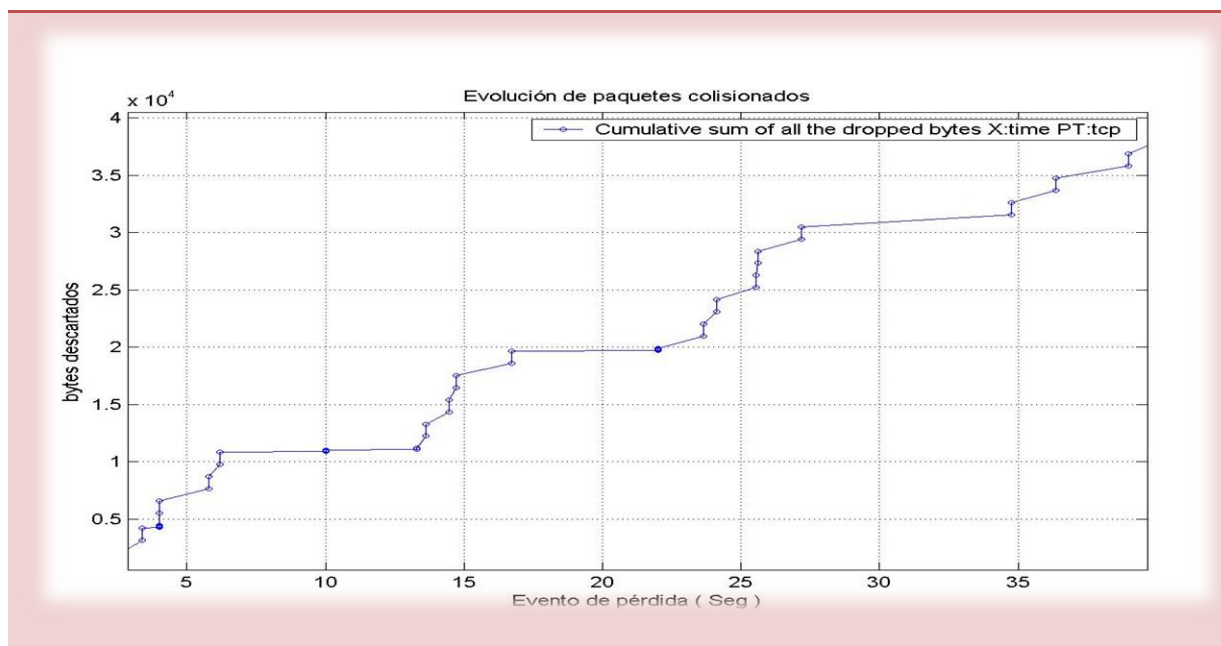


FIGURA 30 EVOLUCIÓN TEMPORAL 4

Como podemos observar tras los resultados obtenidos, el mecanismo de ventana de contención y tiempo de backoff permiten gestionar las colisiones que se producen en la red.

En la simulación vemos que el valor que limita las colisiones es el de CW_{min} , cuanto mayor sea este indicador, tras una colisión el nodo emisor esperará un tiempo mayor o menor para volver a comenzar la retransmisión.

Con valores bajos, como vemos en las figuras 26 y 30, donde $CW_{min} = 2$, el tiempo de espera para la primera retransmisión es muy bajo, produciendo en la mayoría de casos una nueva colisión.

En la figura 30 podemos observar la evolución de los bytes descartados por la red debido a colisiones derivadas de una ventana de contención ineficiente.

En el caso opuesto, un valor de la ventana de contención muy alto (400 unidades) ofrece una tasa de pérdida de paquetes baja, debido a la espera que hace el nodo emisor antes de volver a retransmitir el paquete colisionado. Como consecuencia de este beneficio en la eficiencia de pérdida de paquetes, cabe destacar que debido a la espera tras una colisión, la eficiencia de la red disminuye debido al compromiso entre las colisiones de la red y los paquetes enviados a los nodos receptores.

8.2. THROUGHPUT Y GOODPUT

A continuación se realizara el estudio del Througput y Goodput de la red generada, estudiando los parámetros que definen el acceso y el control de colisiones.

Troughput[2][1]

Se define como la tasa promedio de transferencia de datos por unidad de tiempo, en nuestro caso de estudio nos centraremos en la tasa promedio de paquetes TCP.

El throughput de nuestra red creada incluye los paquetes retransmitidos debido a colisiones así como las cabeceras de cada paquete enviado.

Goodput[2][1]

Definimos el goodput de una red como la tasa efectiva promedio de transferencia de datos por unidad de tiempo.

El goodput no incluye los paquetes retransmitidos debido a descarte o colisiones ni el tamaño de cabeceras.

Por ello se emplea la definición de goodput como la medida en bits/segundo para estudiar la eficiencia de una red.

8.3. SLOT TIME

Como hemos definido anteriormente según el estándar 802.11 IEEE un slot time conlleva el tiempo que el transmisor comprueba que el medio se encuentra libre de colisiones y es el tiempo en el cual puede iniciar su transmisión.

A continuación se describen los tres casos de estudio para el tiempo de *time slot*.

Se estudiará la eficiencia de la red a nivel de Goodput para diferentes valores de *slot time*.

En las gráficas siguientes vemos representados los valores a lo largo del tiempo del goodput y throughput de la línea, para los diferentes valores de *time slot* quedando representadas por los siguientes conceptos.

- Eje de ordenadas: evolución temporal de la simulación.
- Eje de abscisas: throughput de la línea.
- Throughput of receiving bits: goodput de la línea.
- Throughput of generating bits: throughput de la línea.

Slot Time 2 microsegundos

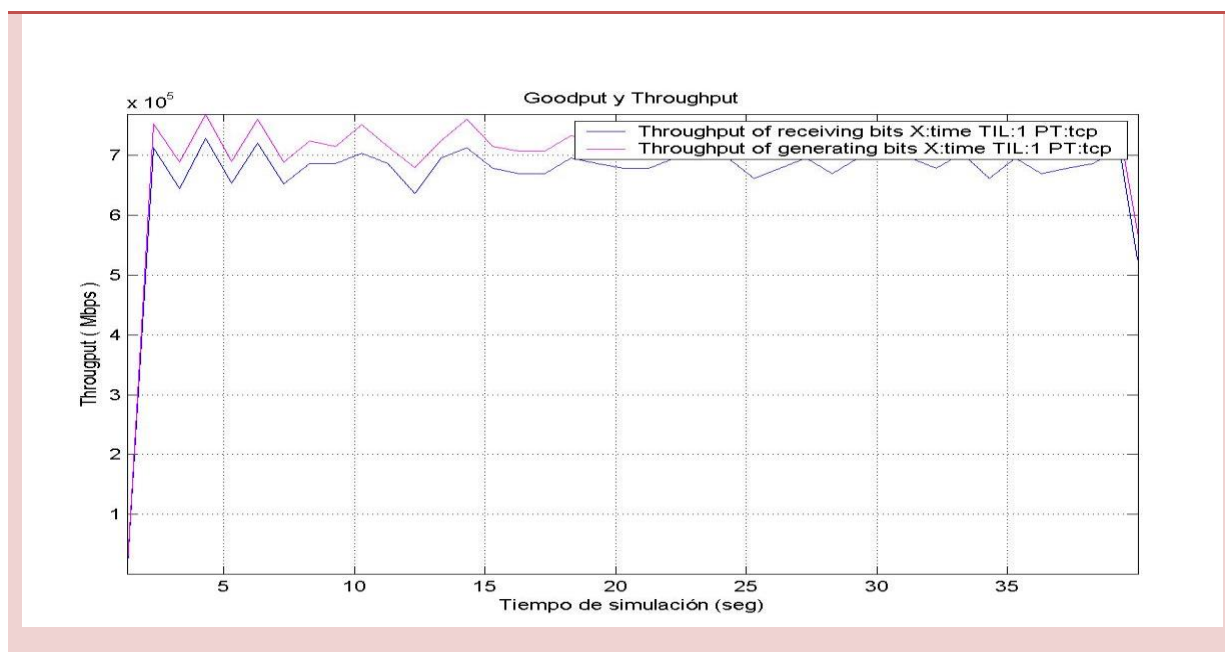


FIGURA 31 EFICIENCIA SLOT TIME

En la figura 31, se emplea un *time slot* de 2 μ s, el cual es determinado por el estándar 802.11 [7][3].

En la gráfica resultante, vemos la comparativa entre el goodput y el throughput de la red, determinados por dicho valor de *time slot*.

La configuración de un *time slot*, con un valor de 2 μ s, permite que las estaciones transmisoras puedan comenzar su transmisión en intervalos temporales más consecutivos, permitiendo así un mayor número de paquetes generados por unidad de tiempo.

A continuación se detallan dos casos para los cuales el intervalo de tiempo de transmisión se aumenta, viendo su repercusión en el goodput efectivo de la red.

Slot Time 8 microsegundos

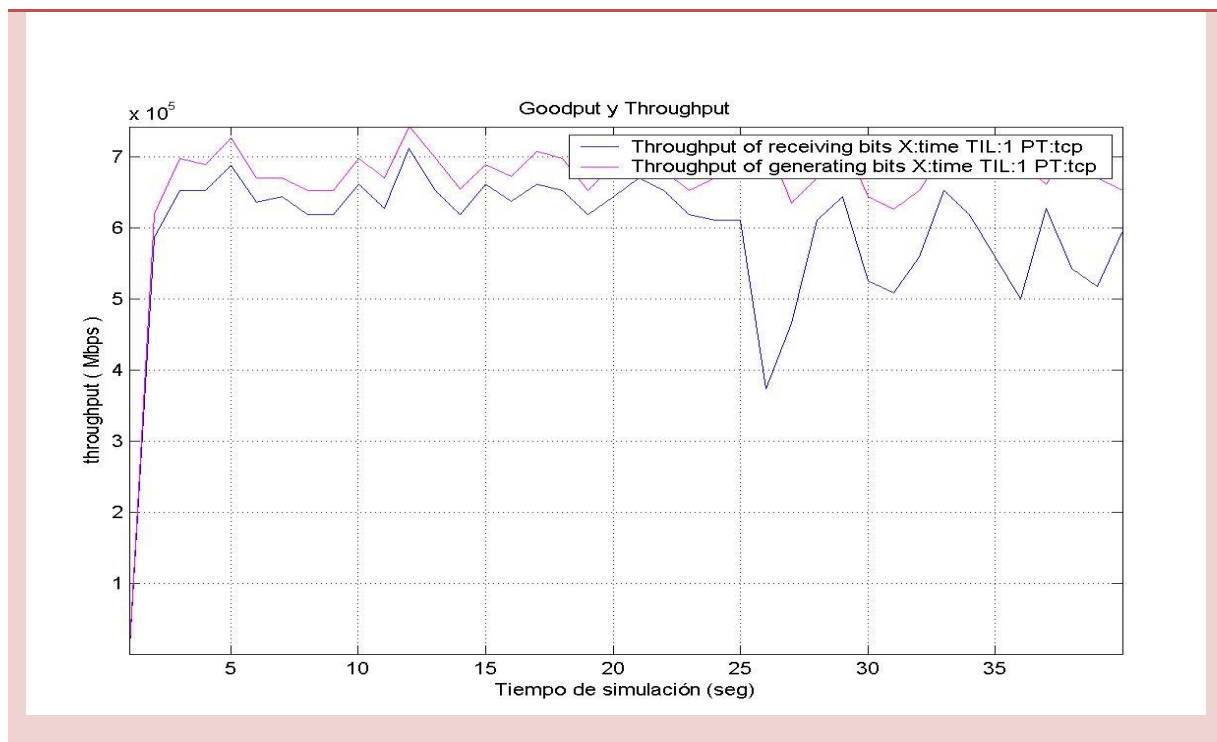


FIGURA 32 EFICIENCIA SLOT TIME 2

Slot Time 10 microsegundos

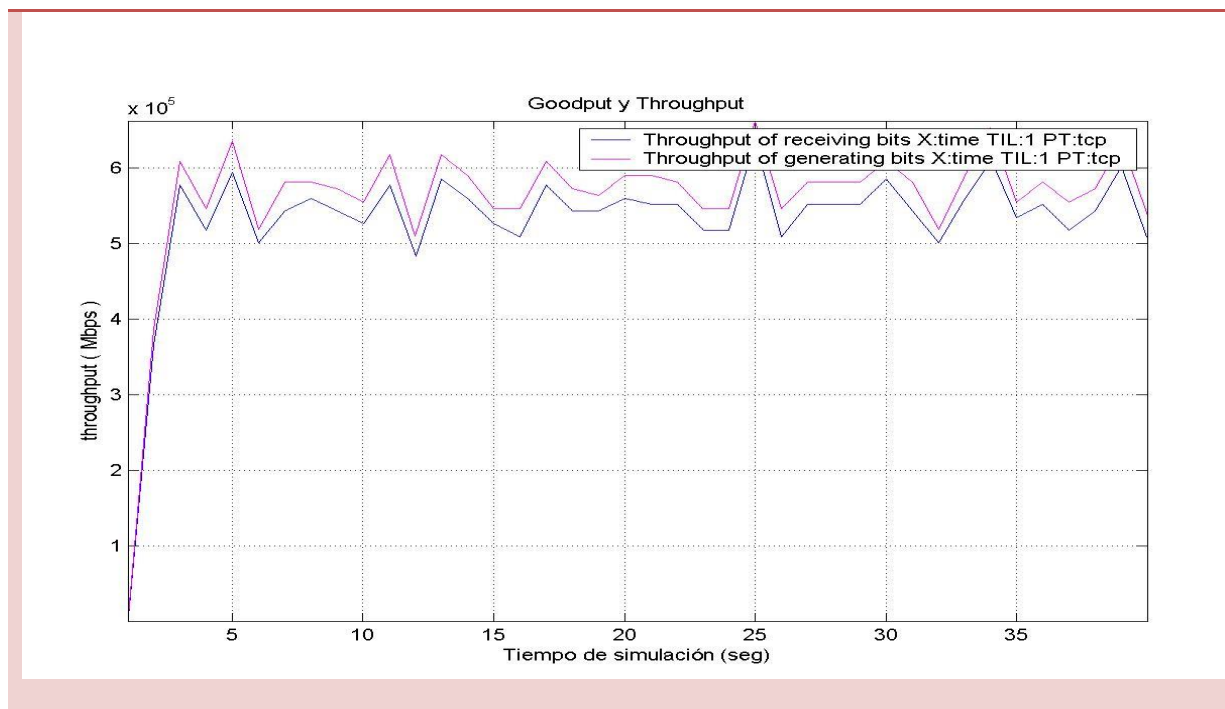


FIGURA 33 EFICIENCIA SLOT TIME 3

Como se puede observar en las figuras 32 y 33, al aumentar el intervalo de slot, la tasa efectiva, que viene determinada por la relación entre el número de paquetes enviados satisfactoriamente por unidad de tiempo, disminuye, debido a que existen menores periodos para que las estaciones transmisoras puedan comenzar el intercambio de paquetes.

Otra consecuencia derivada de un periodo de slot time superior al que determina el estándar 802.11, implica que en redes que se encuentren saturadas, los mecanismos de Backoff descritos anteriormente, no puedan realizar correctamente la función de descongestionar la red, produciendo como consecuencia que los nodos transmisores descarten los paquetes entrantes debido a que su buffer de transmisión se desborde.

A continuación se muestra la evolución del Goodput o tasa efectiva de la red generada, variando el parámetro *Slot Time*.



FIGURA 34 COMPARATIVA SLOT TIME

Como podemos observar existe una disminución de la tasa efectiva a medida que aumenta el valor de *Slot Time* debido a la disminución del intervalo que las estaciones transmisoras disponen para realizar la transmisión de paquetes o aplicar las técnicas de contienda en el caso de que se produzcan colisiones.

8.4. SIFS (SHORT INTERFRAME SPACE)

A continuación se estudiará la eficiencia de la red en función del parámetro SIFS que se define como el tiempo de espera para la generación de paquetes prioritarios, tales como tramas RTS/CTS y el envío de las confirmaciones o ACK's.

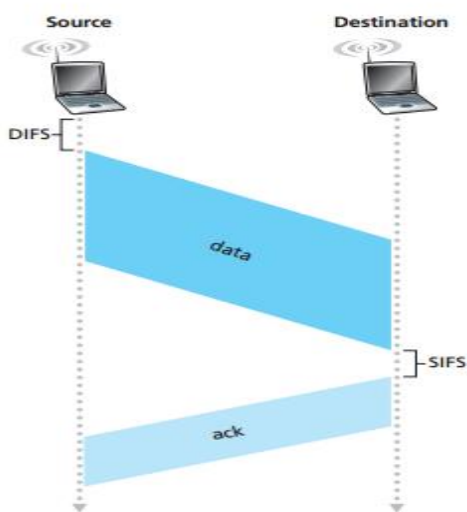


FIGURA 35 RELACIONES TEMPORALES

Cuando una estación comprueba que el canal se encuentra libre (idle), esta transmite la trama tras esperar un periodo de tiempo denominado DIFS (Distributed interframe space).

Una vez esperado este tiempo, se envía la trama esperando que la estación receptora devuelva el asentimiento.

Para evitar el problema de colisiones debido a que otra estación envíe datos durante la espera de este tiempo SIFS, se emplean las tramas RTS y CTS que sirven para reservar el acceso al canal.

Una vez que el receptor recibe el paquete, envía una trama RTS para indicar que necesita el canal para enviar confirmación de trama recibida.

A su vez, se envía la trama broadcast CTS para indicar a las demás estaciones que el medio está reservado para otra estación, evitando así las colisiones.

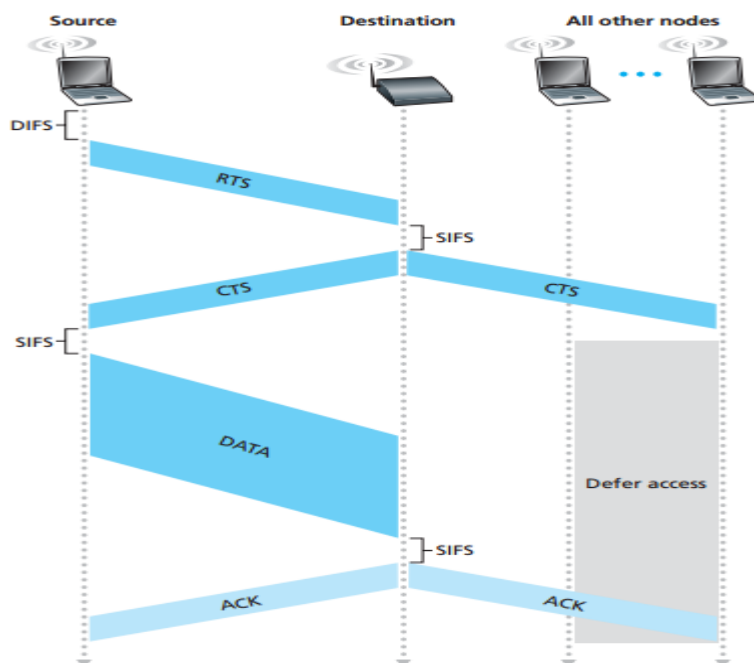


FIGURA 36 RELACIONES TEMPORALES 2

A continuación se muestra la evolución de la eficiencia de la red, derivada de las colisiones producidas en las tramas ACK generadas por la estación receptora.

Mediante la modificación del tiempo SIFS observaremos la evolución de la tasa efectiva de la red inalámbrica.

El valor prefijado en la simulación para el estándar 802.11 del tiempo SIFS es de 1 microsegundo, se aumentará progresivamente para observar la pérdida de eficiencia generada por el retardo en el envío de los asentimientos así como las tramas de reserva del canal RTS y CTS

A continuación observamos el resultado de las simulaciones, aumentando el tiempo SIFS, vemos la disminución progresiva de la eficiencia de la red debido a un mayor tiempo por parte del receptor en reservar el canal para la confirmación de las tramas, generándose así colisiones y sus respectivas retransmisiones.

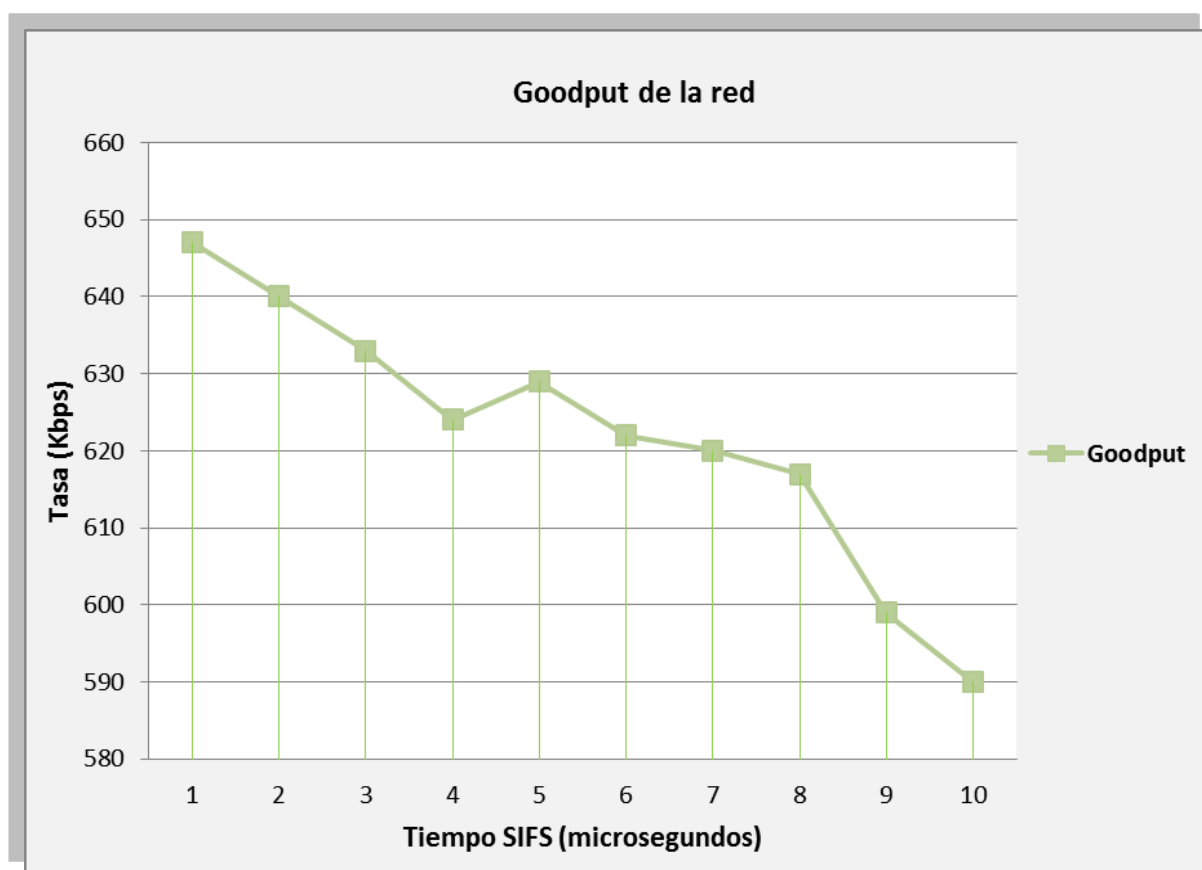


FIGURA 37 COMPARATIVA SIFS

8.5. NÚMERO DE USUARIOS

Una vez estudiada la influencia de los parámetros que regulan el acceso al medio así como la gestión de las colisiones, procederemos a realizar el estudio de la eficiencia de la red inalámbrica generada en función del número de los usuarios que acceden al sistema.

Los resultados de las simulaciones se compararán con la eficiencia teórica que proporciona el protocolo CSMA.

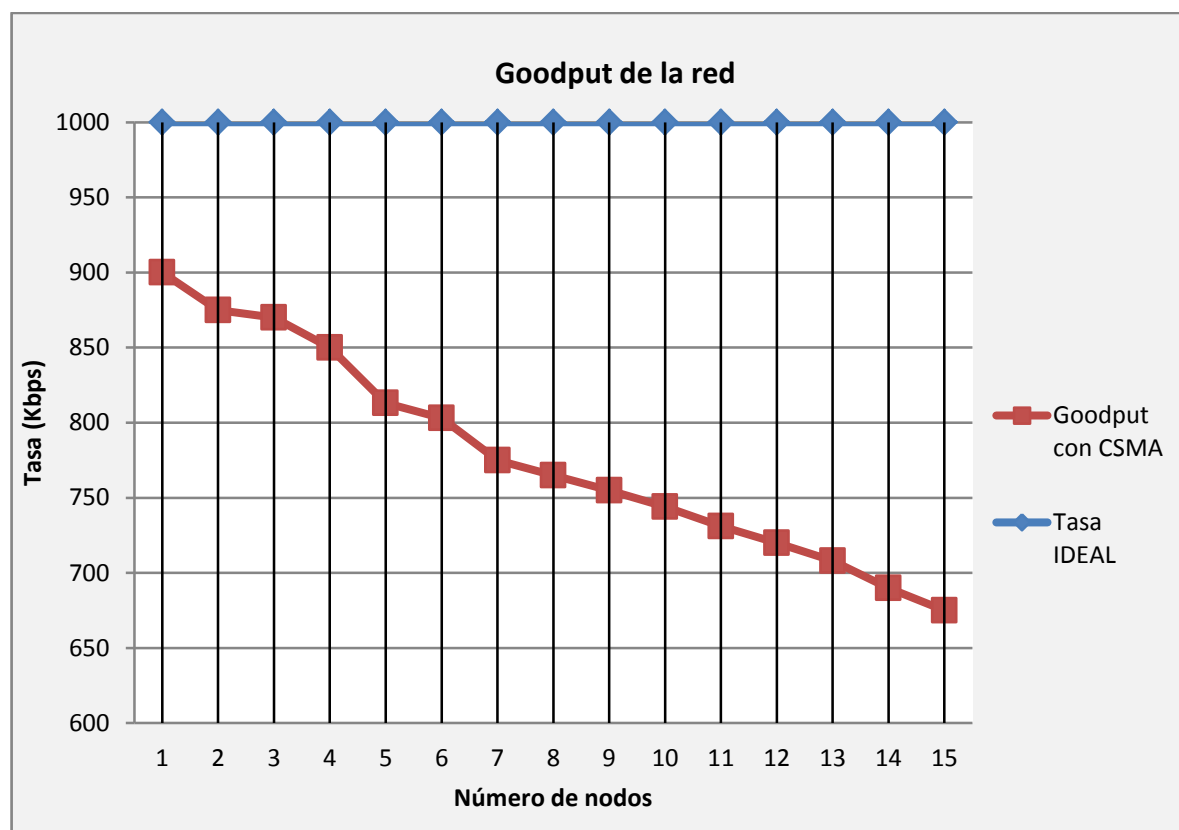


FIGURA 38 COMPARATIVA NÚMERO DE USUARIOS

La figura 38 muestra la evolución del Goodput de la red simulada en función del número de usuarios que se encuentran en el sistema.

- El eje de ordenadas muestra la tasa efectiva del sistema para un número de usuarios determinado.
- El eje de abscisas muestra el número de usuarios que se encuentran en el sistema.

Como se puede observar, existe para el modelo simulado, un descenso del Goodput de la línea a medida que aumenta el número de usuarios, debido al número de retransmisiones que se generan al aumentar las colisiones de paquetes en la red.

Como comparativa adicional se muestra la tasa ideal del enlace, en el caso de que existiera plena capacidad para el envío de datos y no existieran colisiones.

Posteriormente se emplearán estos resultados obtenidos en la simulación, mediante el software NS2 para comparar con los resultados teóricos proporcionados por el modelo de Giuseppe Bianchi[8].

Eficiencia de la red (Throughput Vs Descarte de paquetes)

7 estaciones transmisoras

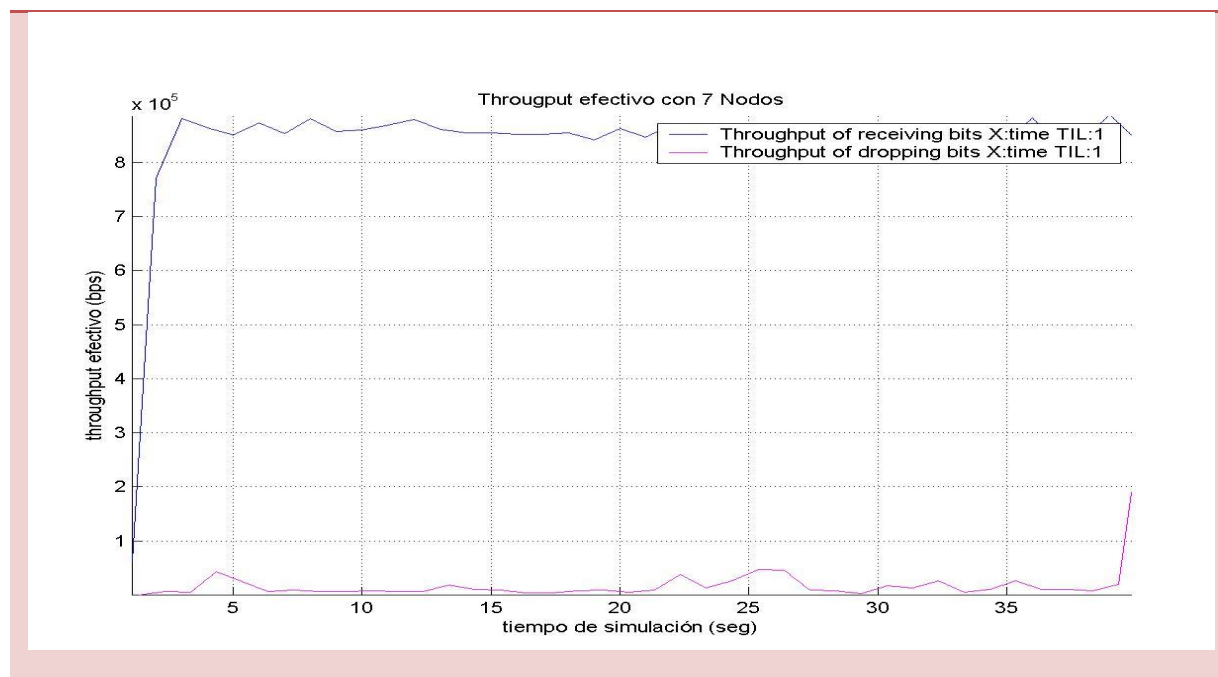


FIGURA 39 EFICIENCIA 7 ESTACIONES

En la figura 39 se muestra la evolución del goodput y la tasa de descarte de paquetes de la línea, en función del tiempo de la simulación.

Se puede observar cómo el protocolo CSMA permite mantener constante en valores bajos, la tasa de descarte de paquetes.

15 estaciones transmisoras

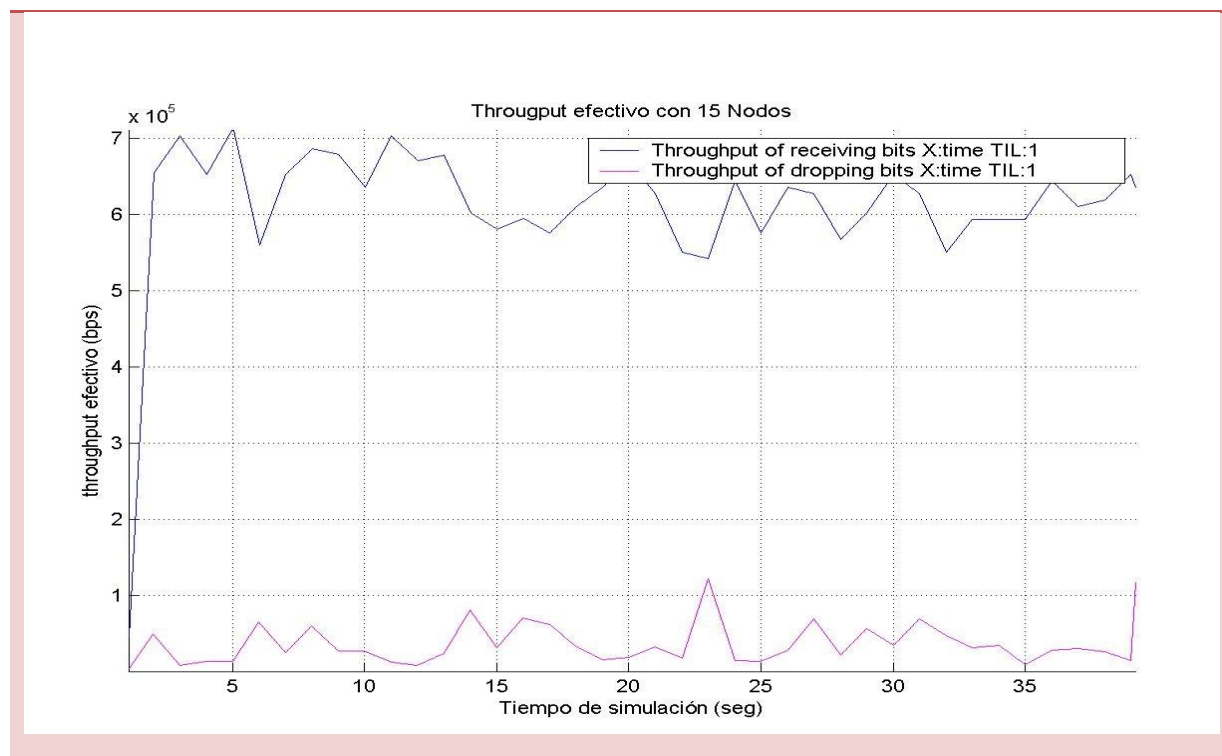


FIGURA 40 EFICIENCIA 15 ESTACIONES

En la figura 40 podemos observar que al introducir 15 estaciones transmisoras, el goodput de la línea disminuye, existiendo variaciones bruscas, debido a la congestión de la red.

Se puede observar a su vez cómo la tasa de descarte de paquetes aumenta y no muestra una tendencia constante como el caso descrito anteriormente, donde compartían el canal 7 usuarios.

Esto se debe a que la red comienza a sobrecargarse, existiendo un mayor número de colisiones y el protocolo CSMA trata de contener la congestión de la línea.

Podemos observar en la figura 40 la comparación entre la velocidad ideal de la red en función del número de usuarios y la velocidad cursada empleando el protocolo CSMA.

Entre 2 y 7 usuarios vemos que la técnica del algoritmo de *back off* y el empleo de una ventana de contención adecuada permite resolver las colisiones que ocurren en la red, ofreciendo una tasa efectiva por usuario constante.

En el caso de que la red inalámbrica aumente el número de usuarios que acceden a ella, vemos una disminución brusca de las prestaciones, apareciendo una saturación en el enlace debido a las múltiples colisiones que ocurren.

8.6. COMPARATIVA DE MODELO TEÓRICO Y SIMULADO

Tras haber descrito el modelo teórico, basado en el algoritmo de Bianchi [8], se procederá a comparar los resultados obtenidos en la simulación con los resultados teóricos.

La comparativa a continuación descrita hace referencia al goodput de la línea en función del número de usuarios que acceden al canal.

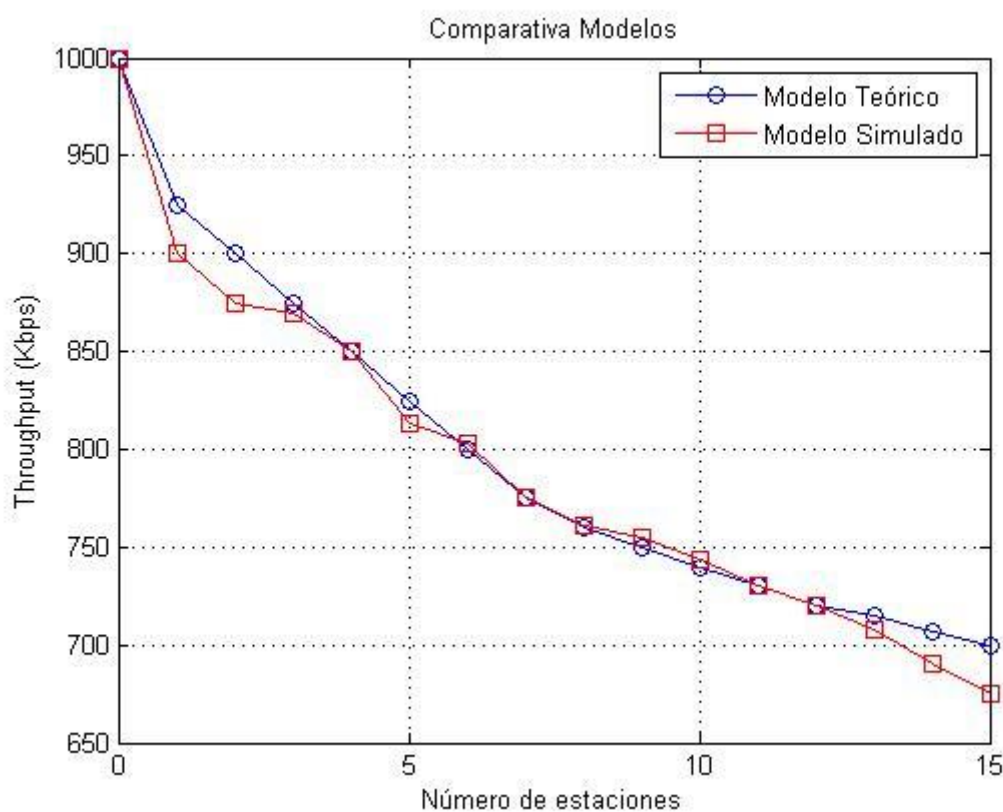


FIGURA 41 COMPARATIVA MODELOS

En la figura 41, se muestra la comparativa del goodput de la línea en función del número de usuarios.

Podemos apreciar que el modelo teórico sigue una pérdida de tasa efectiva más lineal que el modelo simulado a pesar de que los dos modelos se ajustan claramente.

La tendencia del modelo simulado, es debida a la distribución de la topología de la red, ya que la disposición de las estaciones transmisoras, sigue una distribución aleatoria.

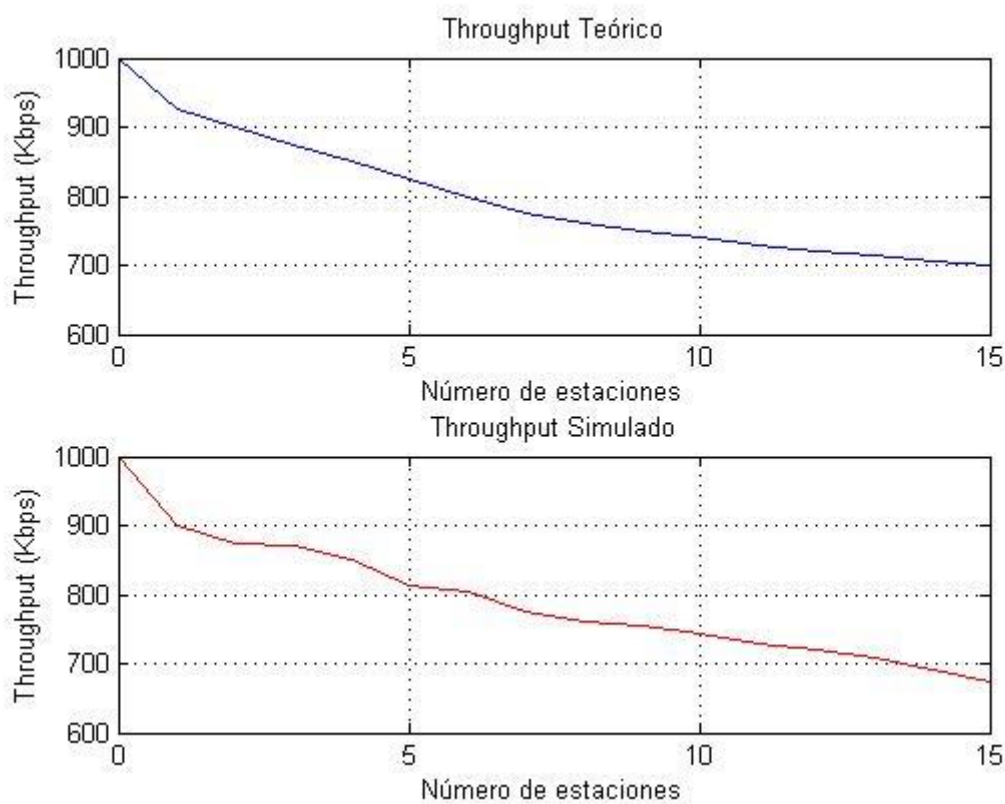


FIGURA 42 COMPARATIVA MODELOS 2

Número de usuarios	Modelo Teórico (Kbps)	Modelo Simulado (Kbps)	Diferencia (Kbps)
1	925	900	25
2	900	875	25
3	875	870	5
4	850	850	0
5	825	813	12
6	800	803	3
7	775	775	0
8	760	765	5
9	750	755	5
10	740	744	4
11	730	731	1
12	720	720	0
13	715	708	7
14	707	690	17
15	700	675	25
Valor medio	781	775	6,37

9. CONCLUSIONES

El trabajo llevado a cabo, ha sido motivado por el objetivo de comprender el funcionamiento real de un sistema de comunicaciones inalámbrico, como es WIFI y permitiendo mediante herramientas especializadas en redes telemáticas, modificar los parámetros fundamentales que rigen el acceso al medio.

El trabajo se ha dividido en cuatro bloques fundamentales,

- Estudio teórico.
- Modelado teórico.
- Simulación mediante software NS2.
- Comparativa de modelos.

Se ha realizado un profundo análisis, basado en el estándar 802.11 WIFI [1] de los parámetros que rigen y determinan el acceso bajo el protocolo CSMA.

El estudio teórico, me ha permitido comprender y determinar, cuales son los aspectos más significativos de la norma 802.11 y el protocolo de acceso al medio CSMA, para abarcarlos posteriormente en las simulaciones y así permitir analizar los resultados obtenidos bajo una base sólida.

Las simulaciones, han sido llevadas a cabo para determinar la correlación entre los modelos que se exponen a nivel teórico sobre las prestaciones de la red inalámbrica WIFI.

Mediante el software especializado en redes telemáticas NS2, se ha podido comprobar y simular, el modelo real de una red WIFI, permitiendo en amplio detalle, configurar y modificar los parámetros que regulan e intervienen en las prestaciones del protocolo CSMA.

Como parte final del trabajo, la conclusión del estudio, reside en la comparativa entre los modelos teóricos y simulado, donde podemos apreciar que ambos modelos tienen una elevada correlación en sus resultados, quedando definida, la influencia de parámetros del protocolo CSMA en las prestaciones globales de la red.

Gracias a las simulaciones, se permite apreciar en qué situaciones es viable derivar tráfico de una red móvil, la cual tiene sobrecarga de tráfico, a una red WIFI, la cual puede ser modificada a nivel de protocolo de la capa de acceso, para permitir un mayor número de usuarios, un mayor throughput de la línea o una robustez mayor para poder cursar el tráfico extra recibido.

10. TRABAJO FUTURO

Los siguientes objetivos no se han contemplado y se proponen como trabajo futuro.

- Realizar una comparativa entre las diferentes versiones del estándar 802.11 IEEE.
- Investigar posibles deficiencias del estándar 802.11 IEEE.

Comparar los diferentes protocolos de acceso al medio:

- Protocolos de asignación fija.
- Protocolos de contienda.

Estudiar las condiciones sobre las cuales se pretende derivar tráfico de redes móviles a la red WIFI.

- Estudio de los factores que influyen en la sobrecarga de redes móviles.
- Estudio de las prestaciones de redes móviles UMTS/LTE
- Simulación real del handover de usuarios entre red móvil y red WIFI.

11. BIBLIOGRAFÍA

- [1] I. Standard, IEEE Std. 802.11, 2012.
- [2] G. Bianchi, «Performance Analysis of the IEEE 802.11 Distributed Coordination Function,» *IEEE Journal on Selected Areas in Communications*, vol. 18, 2000.
- [3] «The Network Simulator,» [En línea]. Available: <http://www.isi.edu/nsnam/ns/>.
- [4] A. S. Tanenbaum, *Redes de computadoras*, Prentice- Hall, 1997.
- [5] J. F. K. K. W. Ross, *Computer Networking*, Addison Wesley, 2001.
- [6] I. Standard, «DCF Access Procedure,» de *IEEE Standard 802.11*, 2012.
- [7] I. Standard, «IFS Relationships,» de *IEEE Standard 802.11*, 2012.
- [8] I. Standard, «MAC sublayer functional description,» de *IEEE Standard 802.11*, 2012.
- [9] I. Standard, «DCF timing relations,» de *IEEE Standard*, 2012.
- [10] E. Altman, *NS Simulator for Beginners*, 2012.
- [11] O. M. Bonastre, «Introducción a la programación de protocolos con NS2,» Editorial Club Universitario.
- [12] UC3M, «Instalación de NS2 en Windows,» [En línea]. Available: <http://www.it.uc3m.es/rcalzada/ns/windows/>.
- [13] S. O. E. E. & C. Science, «Introduction to Network Simulator».
- [14] M. Greis, «Tutorial for the network simulator "ns"».

12. ANEXOS

12.1. CÓDIGO DE LA SIMULACIÓN.

```
10. #
11. #####
12. # Analisis de las prestaciones del acceso al medio CSMA en redes WIFI
13. # Código acceso_csma.tcl
14. # Autor: Ávaro Arnanz Arroyo
15. # Trabajo final de Grado
16. #
17. #####
18. # Definimos las opciones del canal inalámbrico
19. setval(chan) Channel/WirelessChannel ;
20. setval(prop) Propagation/TwoRayGround ;
21. setval(netif)Phy/WirelessPhy ;
22. set val(mac) Mac/802_11 ;
23. set val(ifq)Queue/DropTail/PriQueue ;
24. set val(ll) LL ;
25. setval(ant) Antenna/OmniAntenna ;
26. set val(ifqlen)50 ;
27. set val(num_nodos)15 ;
28. set val(rp) DSDV ;
29. set val(x)300 ;
30. set val(y)300 ;
31. set val(stop)40
32.
33. #Creamos objeto de tipo simulador
34. setns[new Simulator]
35.
36. #Definimos las opciones del estandar 802.11
37.
38. #Ventana de contención
39. $val(mac) set CWMin_ 15
40. $val(mac) set CWMax_ 1024
41.
42. #Duración del slot-time
43. $val(mac) set SlotTime_ 0.000020
44.
45. #Espacio entre tramas para paquetes de alta prioridad
46. $val(mac) set SIFS_ 0.000010
47. $val(mac) set ShortRetryLimit_ 7
48. $val(mac) set LongRetryLimit_ 4
49. Agent/DSDV set perup_ 15000000 ;
50.
51. # Tasa binaria del enlace en Mbps
52. Mac/802_11 set dataRate_ 1.0e6
53.
54. # Definir objetos de resultados traza
```

```
55. settracefd[open csma.tr w]
56. setnamtrace[open csma.nam w]
57.
58. $ns trace-all $tracefd
59. $nsnamtrace-all-wireless $namtrace $val(x) $val(y)
60.
61. # Definir la topografía del escenario
62. set topo [new Topography]
63. #Asignar variables de tamaño
64.
65. $topoload_flatgrid $val(x) $val(y)
66. #Generamos los nodos definidos
67. create-god $val(num_nodos)
68.
69. # Creamos las características de los nodos y los introducimos en el
    escenario
70.
71. # Configuración general de los nodos
72. $ns node-config-adhocRouting $val(rp) \
73. -llType $val(ll) \
74. -macType $val(mac) \
75. -ifqType $val(ifq) \
76. -ifqLen $val(ifqlen) \
77. -antType $val(ant) \
78. -propType $val(prop) \
79. -phyType $val(netif) \
80. -channelType $val(chan) \
81. -topoInstance $topo \
82. -agentTrace OFF \
83. -routerTrace OFF \
84. -macTrace ON \
85. -movementTrace OFF
86.
87. for{seti 0}{ $i < $val(num_nodos) }{incr i}{
88. set node_($i) [$ns node]
89.
90.
91. }
92.
93. # Posición inicial de los nodos
94.
95. $node_(0) set X_ 5.0
96. $node_(0) set Y_ 100.0
97. $node_(0) set Z_ 0.0
98.
99. # Crea los nodos en la cuadrícula
100. for{seti 1}{ $i < $val(num_nodos) }{incr i}{
101.
102. $node_($i) set X_ [expr rand()*$val(x)]
103. $node_($i) set Y_ [expr rand()*$val(y)]
104. $node_($i) set Z_ 0
105. }
106.
107. # Asignar tráfico de nodo origen
108. settcp[new Agent/TCP/Newreno]
```

```
109. $tcp set class_ 2
110. set tcp2 [new Agent/TCP/Newreno]
111. $tcp2 set class_ 2
112. set tcp3 [new Agent/TCP/Newreno]
113. $tcp3 set class_ 2
114. set tcp4 [new Agent/TCP/Newreno]
115. $tcp4 set class_ 2
116. set tcp5 [new Agent/TCP/Newreno]
117. $tcp5 set class_ 2
118. set tcp6 [new Agent/TCP/Newreno]
119. $tcp6 set class_ 2
120. set tcp7 [new Agent/TCP/Newreno]
121. $tcp6 set class_ 2
122. set tcp8 [new Agent/TCP/Newreno]
123. $tcp6 set class_ 2
124. set tcp9 [new Agent/TCP/Newreno]
125. $tcp6 set class_ 2
126. set tcp10 [new Agent/TCP/Newreno]
127. $tcp6 set class_ 2
128. set tcp11 [new Agent/TCP/Newreno]
129. $tcp6 set class_ 2
130. set tcp12 [new Agent/TCP/Newreno]
131. $tcp6 set class_ 2
132. set tcp13 [new Agent/TCP/Newreno]
133. $tcp6 set class_ 2
134. set tcp14 [new Agent/TCP/Newreno]
135. $tcp6 set class_ 2
136. set tcp15 [new Agent/TCP/Newreno]
137. $tcp6 set class_ 2
138.
139. # Asignar tráfico de nodo destino
140. set sink [new Agent/TCPSink]
141. $nsattach-agent$node_(0)$tcp
142. $nsattach-agent$node_(1)$sink
143. $nsconnect$tcp$sink
144. set sink2 [new Agent/TCPSink]
145. $nsattach-agent$node_(1)$tcp2
146. $nsattach-agent$node_(2)$sink2
147. $nsconnect$tcp2$sink2
148. set sink3 [new Agent/TCPSink]
149. $nsattach-agent$node_(2)$tcp3
150. $nsattach-agent$node_(3)$sink3
151. $nsconnect$tcp3$sink3
152. set sink4 [new Agent/TCPSink]
153. $nsattach-agent$node_(3)$tcp4
154. $nsattach-agent$node_(1)$sink4
155. $nsconnect$tcp4$sink4
156. set sink5 [new Agent/TCPSink]
157. $nsattach-agent$node_(4)$tcp5
158. $nsattach-agent$node_(3)$sink5
159. $nsconnect$tcp5$sink5
160. set sink6 [new Agent/TCPSink]
161. $nsattach-agent$node_(5)$tcp6
162. $nsattach-agent$node_(3)$sink6
163. $nsconnect$tcp6$sink6
```



```
164. set sink7 [new Agent/TCPSink]
165. $nsattach-agent$node_ (6) $tcp7
166. $nsattach-agent$node_ (4) $sink7
167. $nsconnect$tcp7$sink7
168. set sink8 [new Agent/TCPSink]
169. $nsattach-agent$node_ (6) $tcp8
170. $nsattach-agent$node_ (3) $sink8
171. $nsconnect$tcp8$sink8
172. set sink9 [new Agent/TCPSink]
173. $nsattach-agent$node_ (4) $tcp9
174. $nsattach-agent$node_ (8) $sink9
175. $nsconnect$tcp9$sink9
176. set sink10 [new Agent/TCPSink]
177. $nsattach-agent$node_ (9) $tcp10
178. $nsattach-agent$node_ (7) $sink10
179. $nsconnect$tcp10$sink10
180. set sink11 [new Agent/TCPSink]
181. $nsattach-agent$node_ (5) $tcp11
182. $nsattach-agent$node_ (6) $sink11
183. $nsconnect$tcp11$sink11
184. set sink12 [new Agent/TCPSink]
185. $nsattach-agent$node_ (11) $tcp12
186. $nsattach-agent$node_ (7) $sink12
187. $nsconnect$tcp12$sink12
188. set sink13 [new Agent/TCPSink]
189. $nsattach-agent$node_ (10) $tcp13
190. $nsattach-agent$node_ (1) $sink13
191. $nsconnect$tcp13$sink13
192. set sink14 [new Agent/TCPSink]
193. $nsattach-agent$node_ (12) $tcp14
194. $nsattach-agent$node_ (13) $sink14
195. $nsconnect$tcp14$sink14
196. set sink15 [new Agent/TCPSink]
197. $nsattach-agent$node_ (14) $tcp15
198. $nsattach-agent$node_ (8) $sink15
199. $nsconnect$tcp15$sink15
200.
201. # Definir interconexiones entre nodos
202. set ftp [new Application/Traffic/CBR]
203. $ftpattach-agent$tcp
204. $ftp set packetSize_ 1444
205. $ftp set interval_ 0.05000
206. $ns at 1.0 "$ftp start"
207. $ns at 40 "$ftp stop"
208. set f [new Application/Traffic/CBR]
209. $fattach-agent$tcp2
210. $f set packetSize_ 1444
211.
212. $f set interval_ 0.05000
213. $ns at 1.0 "$f start"
214. $ns at 40 "$f stop"
215. set g [new Application/Traffic/CBR]
216. $gattach-agent$tcp3
217. $g set packetSize_ 1444
218.
```

```
219. $g set interval_ 0.05000
220. $ns at 1.0"$g start"
221. $ns at 40"$g stop"
222. set h [new Application/Traffic/CBR]
223. $hattach-agent$tcp4
224. $h set packetSize_ 1444
225.
226. $h set interval_ 0.05000
227. $ns at 1.0"$h start"
228. $ns at 40"$h stop"
229. set i [new Application/Traffic/CBR]
230. $iattach-agent$tcp5
231. $i set packetSize_ 1444
232.
233. $i set interval 0.05000
234. $ns at 1.0"$i start"
235. $ns at 40"$i stop"
236. set j [new Application/Traffic/CBR]
237. $jattach-agent$tcp6
238. $j set packetSize_ 1444
239.
240. $j set interval_ 0.05000
241. $ns at 1.0"$j start"
242. $ns at 40"$j stop"
243.
244. set k [new Application/Traffic/CBR]
245. $kattach-agent$tcp7
246. $k set packetSize_ 1444
247.
248. $k set interval_ 0.05000
249. $ns at 1.0"$k start"
250. $ns at 40"$k stop"
251. set l [new Application/Traffic/CBR]
252. $lattach-agent$tcp8
253. $l set packetSize_ 1444
254.
255. $l set interval_ 0.05000
256. $ns at 1.0"$l start"
257. $ns at 40"$l stop"
258. set m [new Application/Traffic/CBR]
259. $mattach-agent$tcp9
260. $m set packetSize_ 1444
261.
262. $m set interval_ 0.05000
263. $ns at 1.0"$m start"
264. $ns at 40"$m stop"
265. set n [new Application/Traffic/CBR]
266. $nattach-agent$tcp10
267. $n set packetSize_ 1444
268.
269. $n set interval_ 0.05000
270. $ns at 1.0"$n start"
271. $ns at 40"$n stop"
272. set o [new Application/Traffic/CBR]
273. $oattach-agent$tcp11
```

```
274. $o set packetSize_ 1444
275.
276. $o set interval_ 0.05000
277. $ns at 1.0"$o start"
278. $ns at 40"$o stop"
279. set p [new Application/Traffic/CBR]
280. $pattach-agent$tcp12
281. $p set packetSize_ 1444
282.
283. $p set interval_ 0.05000
284. $ns at 1.0"$p start"
285. $ns at 40"$p stop"
286. set q [new Application/Traffic/CBR]
287. $qattach-agent$tcp13
288. $q set packetSize_ 1444
289.
290. $q set interval_ 0.05000
291. $ns at 1.0"$q start"
292. $ns at 40"$q stop"
293. set r [new Application/Traffic/CBR]
294. $rattach-agent$tcp14
295. $r set packetSize_ 1444
296.
297. $r set interval_ 0.05000
298. $ns at 1.0"$r start"
299. $ns at 40"$r stop"
300. set s [new Application/Traffic/CBR]
301. $sattach-agent$tcp15
302. $s set packetSize_ 1444
303.
304. $s set interval_ 0.05000
305. $ns at 1.0"$s start"
306. $ns at 40"$s stop"
307.
308.
309.
310. # Define posición para la representación animada
311. for{seti0}{$i<$val(num_nodos)}{incri}{
312. # 30 defines the node size for nam
313. $nsinitial_node_pos$node_($i)30
314. }
315.
316. # Condición de parada
317. for{seti0}{$i<$val(num_nodos)}{incri}{
318. $ns at $val(stop)"$node_($i) reset";
319. }
320.
321. # endingnam and thesimulation
322. $ns at $val(stop)"$ns nam-end-wireless $val(stop)"
323. $ns at $val(stop)"stop"
324. $ns at 40.1"puts \"fin de la simulacion\" ; $nshalt"
325.
326.
327.
328. proc stop {}{
```



```
329. global nstracefdnamtrace
330. $nsflush -trace
331. close $tracefd
332. close $namtrace
333. # Ejecuta fichero de animación
334. exec namcsma.nam &
335. exit 0
336. }
337. $ns run
```